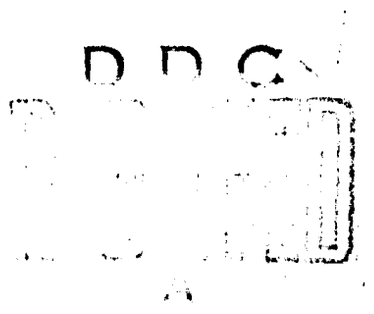
CLASSIFICATION MANAGEMENT



JOURNAL OF THE NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME VII - 1971

Published semiannually. Annual subscription, $10. Editorial address: 14001 Daphne Ave., Gardena, Calif., 90249, Lorimer F. McConnell, Editor. Views expressed by individuals herein do not necessarily represent views of their employers or of NCMS.

CONTENTS

PAPERS FROM THE SEVENTH NATIONAL SEMINAR

KEYNOTE ADDRESS
BY
LT. GENERAL ROBERT E. COFFIN, USA

It is a great pleasure for me to join you this morning to discuss the subject of classification management. You who are engaged in this field are doing work that is vital to safeguarding our nation's security. Your efforts are also contributing significantly to domestic progress in this country by helping to ensure that government-sponsored scientific and technical information can be applied in the broadest possible way to the nonmilitary needs of our society.

In recent years, increased emphasis has been placed on classification management within government, industry and the academic community. Much of the momentum we have seen has come from the positive impact of people like you who are dedicated to professional classification management. Your society's membership comes from many different agencies of government and from industry and the universities. The wide range of professional interest represented by your group is beneficial to both Government and industry in helping to achieve our national goals in classification management.

This morning I want to present some of my views regarding our approach to classification management in research and development. In particular, I will discuss the importance of effectively applying government-sponsored research and development to maintain the overall strength and well-being of the nation — a goal that demands the proper management of security classification.

Finally, I'd like to summarize some of the basic philosophy of the Department of Defense on classification management, set forth our objectives, and show you what we are actually doing to realize them.

The primary goal of classification management is to achieve a suitable balance between the two requirements: safeguarding information that truly needs protection in the interest of national security and, consistent with this mandate, ensuring that there is a maximum flow of information to nondefense areas so that we may realize the benefits of R&D in striving to reach other urgent national objectives.

Today, owing to the scientific and technical revolution that has taken place in recent years, this problem is far more complex than at any time in our history. For instance, during this century, the amount of published findings has doubled about every 8 to 10 years. According to the National Academy of Sciences, every year about 40,000 research papers in physics are published, several times that number in chemistry — and, in all fields of science and technology, perhaps as many as 2 million. And consider also that over 30,000 scientific and technical journals are currently in publication.

As research has grown, science and technology have become increasingly important in government. In the United States, about 60 percent of all research and development is sponsored by the government — much of it related to the needs of our armed forces.

Because of this great Federal involvement in research and development, we who work in the government are responsible for ensuring that our nation is able to reap maximum benefit from technological advances arising from government research programs. This is especially true in defense-related R&D activities, because the measures required to defend this country against military attack are based on much the same technology that is required by industry. There are only a few technologies that are singularly applicable to national security. Science and technology in general can be applied in varying degrees to domestic as well as defense problems.

For these reasons, management of classification plays a vital role in the advantageous use of science and technology in both kinds of national endeavor.

Classification decisions relating to defense R&D are difficult and cannot be based on mathematical calculation. They must rely primarily on the sound judgment of people in classification management and on the cooperation of all government, industry and university people concerned with classified government R&D projects.

Today, fresh Defense emphasis on this matter represents a challenge to classification managers. Especially during the past few years, the DoD has increasingly stressed the need to exercise the best possible judgment and the greatest common sense in the use of security classification for research and development information.

In my opinion, there is a tendency — quite understandable in view of the stakes involved — to overclassify and to continue classification too long. The penalties attached to the release of possibly damaging information are much more severe than the consequences of withholding information that may not be prejudicial to national security. Sometimes, in determining classification, we may have emphasized the possible benefits of the information to potential enemies without fully examining the benefits that could accrue to U.S. and Allied industry through more open and effective technology dissemination. Under present policy on classification, both national security and domestic needs are considered.

The most important considerations in classifying defense R&D information rest on two fundamental needs — to preclude major technological advantages on the part of potential enemies based on our work, and to prevent the disclosure of information that is vital in the development of countermeasures to their weapons or our own. At the same time, current DoD guidance allows for the situation in which the U.S. base of technical competence may be sufficiently broad and deep that we might keep a lead over other nations just as well as in an open race with our competitors as in a secret one.

Now, I want to pose some rhetorical questions that will, I hope, illustrate the classification and security problems that the Department of Defense has been facing for many years. The answers I offer will represent my views on this crucial aspect of Defense R&D management.

Question: How long can we reasonably expect that classified information will remain unknown to potential enemies and thereby preserve U.S. lead time advantage?

Answer: I believe we must accept the fact that certain kinds of technical information are easily discovered by determined investigators. For instance, in spite of the costly and elaborate measures taken by the United States to preserve technical secrecy on its nuclear weapons development — and I do not suggest that we should have handled classification differently — the Soviet Union was not long delayed in developing its own nuclear system.

Obviously, security has limited effectiveness. One might estimate that tightly controlled information will remain secret for a limited number of years. I believe that classification may sometimes be more effective in withholding information from our quiet friends and allies than from highly inquisitive potential enemies.

In view of the limited effectiveness of information control by classification, that control should be retained for the shortest possible time in consideration of the degree to which the information is sensitive, the cost, and the probability of its being compromised in spite of classification.

Question: Granted that some excessive use is being made of classification, what practical steps can be taken to better define the DoD information that should be protected in the interest of national security?

Answer: In considering the answer to this question, we must take into account the effect of controlling Defense information so as to limit its availability to the United States and its allies as compared to the benefits

to potential enemies that would follow its open release.

We are guided by the belief that the long-term interest of our open society, including the speedy exploitation of technological advances, is best served by classifying at minimum levels consistent with the nation's security. In light of that concept, which is basic to DoD philosophy, it may be possible to narrow the span of critical areas that must be protected and still hold to our primary objective of achieving and maintaining a lead over other nations in areas of science and technology that are essential to U.S. security.

Some new and significant DoD classification policies and procedures were established last summer. For every development program supported by the DoD, the sponsoring department or agency must provide guidance concerning, among other things, the security classification of the system's technical characteristics. With respect to major developments for which a Development Concept Paper is required, this guidance on technical characteristics must have the approval of the Director of Defense Research and Engineering, while classification guidance for programs of somewhat less significance will require approval in the sponsoring department or agency at the level of Service Assistant Secretary for Research and Development or his designee. As a related effort, the DDR&E has directed his staff to prepare classification guides in the various technological areas.

Question: Are there key points or milestones in the research, development, production and deployment cycle at which information should be controlled?

Answer: One point that should be carefully considered here is that, if a potential enemy obtains knowledge of our significant research and technology activities, he gains additional lead time that will enable him to predict potential application of our work in weapon systems.

It appears that, in many cases, classification is most critically useful as a means of keeping a technological lead during the period of weapon systems development. In this stage, following design and prior to production, detailed specifications and essential manufacturing techniques are worked out which critically affect system performance. In many cases, the degree of protection required will change when a system becomes operational and its performance becomes evident. If it is decided to revise classification, great care must be taken to prevent the disclosure of vulnerabilities which would enable potential enemies to embark on the early development of specific countermeasures.

Regarding specific phases of the R&D cycle, it appears that little is to be gained by classifying basic research, with which precept DoD policy and practice are already in virtually complete accord. Similarly, I believe that, as a general rule, much early exploratory development could remain unclassified. If classification is required, a specific deadline for declassification should be established.

For all other development work, including advanced exploratory development and advanced development, classifications similar to those we use today are suitable. The criteria governing them, however, should be sharpened to impose classification only to prevent potential enemies from acquiring major technological advantages that could lead to their anticipating and countering our developing activities.

Within the framework of these criteria, the classification of each system, component, subsystem and technique in advanced development should be considered on its own merit. And from the beginning of work in the phases meriting classification, specific schedules of declassification should be imposed.

In any category of classified development, major programmatic changes should be accompanied by the reconsideration of the program's security classification.

Question: Having discussed the philosophical and some of the basic procedural aspects of DoD application of security classification, what should we do to downgrade or declassify the information that we originally believed must be held tightly in the interest of national security? And what have we done so far?

Answer: As our technological knowledge — and that of foreign nations — is more widely diffused, we must review our classified material to determine whether to retain or drop that protection. As you know, current DoD procedures call for automatic downgrading and declassification at intervals of 3 to 12 years, depending on the information's sensitivity. We must be alert to recognize when events and scientific advances make it possible to dispense with classification entirely or reduce it to a lower level.

Security classification guides for DoD contractors, and many of the underlying program guides, have been reviewed for purposes of downgrading or declassifying appropriate elements of information. More than 13,000 guides of this kind were reviewed substantively and in depth. As a result, about 7 percent of them were changed to include downgrading and declassification actions. In one military department alone, 12 contracts and 97 technical orders were entirely declassified, which represents the avoidance of more than a half-million dollars in future costs.

The OSD is also studying a possible blanket declassification of classified information issued before some date in the late 1950s. Particularly sensitive material would naturally have to be excluded, such as intelligence, cryptological information and data on vulnerability, but even that might be downgraded and would be subject to review for declassification.

The very volume of classified material that must be guarded hampers the efforts of our many imaginative people in classification management who could, I am sure, make innovative strides toward a much more thoughtful and effective program if they could be released from considerations of quantity handling to seek qualitative improvements. And I believe that the DoD's recent changes in classification procedures will have the effect of eliminating some of these burdens and the associated costs in the future.

Aside from the benefits of economy and efficiency, however, though they count as important factors, the release of technical information from Defense R&D work would be a boon to scientists and technologists outside the Defense sphere who make innovative contributions to our people's everyday life. The more open we can make our technological programs, the more dynamic will be our national progress in research and development.

Question: All right, what civil benefits can be identified that are derived from DoD's work in science and technology? And would they have been gained eventually even if the Defense findings had not been released to the public?

Answer: Item — The United States' lead in microwave electronics and computer technology was greatly increased after the 1946 decision to release the results of wartime research in those fields. As we all know, computer technology helped get us safely to the moon, and it is predicted that computers and allied industrial work will, in the next 10 years, make the largest contribution to the gross national product of any single industry. Computers are essential tools in much research in educational institutions and private R&D organizations; moreover, they are being used more and more in intensive-care wards of hospitals to monitor patients' life signs and make it possible to save lives that would otherwise be lost.

Item — Once it was decided in the mid-1950s to declassify information in the field of nuclear reactors, research and development in their peaceful uses accelerated remarkably in the United States and other countries as well.

Item — It is highly questionable that

the transistor technology would have developed as successfully as it has in the past 20 years if it had not been the subject of essentially open research. Today, transistors are a part of our daily life.

What delays would have occurred if Defense work in these areas had remained classified and unavailable to the general public? To answer that, we would have to call upon our imaginations to conceive what our situation might have been today if that had happened. So we must remember this recent history in future decisions that will affect the availability of technological information to the nation and the world.

Now, dispensing with the question-and-answer format I have been employing, let me try to summarize:

It is clear that necessary restrictions on the flow of scientific and technical information support and strengthen the security of our nation, but at the same time, exacts the penalty of delaying dissemination to nonmilitary activities of breakthroughs, and scientific advances that Defense R&D has achieved. What the resultant cost to the civil economy is, in terms of manpower and equipment, can't be estimated. Decision on whether to classify or not ultimately should depend on the consequent benefits and penalties to our open democratic society. This presents a dilemma that has to be resolved every time a person looks at a paper and reaches for a classification stamp, or — doesn't reach for it. The answer is based on the needs of the whole country. If we do not properly manage our classification activities, we exact a price from all our people, either through inadequate protection of militarily vital information or through undue delay in the application of scientific advances to our domestic needs.

We must not fail to protect information whose secrecy is crucial to our safety but we can't afford to adopt practices that stifle scientific and technological progress. A sensible path between the two must be found and followed. This is a function of those who work in the field of classification and security.

* * * * *

UPDATING SECURITY CLASSIFICATION MANAGEMENT AND ITS SUPPORT BY DCAS ORGANIZATION

Remarks of George MacClain —

On this part of the program, I am teamed up with Colonel George Zacharias, the Chief of the Office of Industrial Security, Defense Contract Administration Services. As you know, our teamwork is indispensable to objective realization of a successful total Classification Management program.

I want to begin by referring to what Joe Liebling, the Deputy Assistant Secretary of Defense for Security Policy, said last year before this Society when he keynoted our seminar. He said, and I am quoting him now, "Classification Management in the Department of Defense is a responsibility which rests in my office for providing the standards, criteria, procedures, and guidance for identifying information which under statute, executive order, or regulation requires security classification. This responsibility also involves the exercise of management prerogatives to force initiative, consistent with security, for positive, progressive, and complete downgrading and declassification on a timely basis." That definition of Classification Management is one for us to keep in mind through this Seminar, and afterward.

Ladies and gentlemen, this has been a good year for Classification Management. It's been good in a number of different ways. I think of it as good first of all because we have gained recognition in high places beyond anything ever before.

It's been good, too, because we have

achieved a greater degree of expertise and cooperation in both DoD and industry in the development and publication of comprehensive and meaningful classification guidance. I'll cite a few examples of that later on.

It's been a good year also because, we are living together now, more and more, on a very close and cooperative and friendly basis with other elements of the Executive Branch, particularly the National Aeronautics and Space Administration and Atomic Energy Commission, but not to the exclusion of other elements as well. And certainly, within the DoD and its many elements we have gained a great deal in understanding each other's problems, inspiring other elements of DoD to come and see us and to work with us, and we go to them, and we work with them.

And in all of this, of course, I wouldn't want to fail to say at once that we have had especially the continuing cooperation of the Office and organization of Industrial Security headed by George Zacharias. There has been a great deal of emphasis in Classification Management in every one of the eleven Defense Contract Administration Services Regions. Representatives of those Regions are here participating in this Seminar. In every DCASR now, there is a Classification Management official, and these gentlemen fully understand the role they have to play. It is not a role of taking over in any sense the user agency's responsibility for classification guidance all the way. It is, on the other hand, a role of bringing to the attention of these people, and they do it more all the time, problem areas where classification guidance at the contractor level is not adequately provided.

It's been an awfully good year also because of the very important official pronouncements at the level of the OSD. You heard Joe Liebling last year tell you that the Defense Science Board in the Office of the Director of Defense Research and Engineering, and the Director himself, had been very heavily engaged in examining the question of classification in research and development. Last July was too early to predict the outcome. But I can now tell you what actually has been stated at the highest level of DoD policy in this regard.

One of the most important pronouncements is that classification guidance, good classification guidance, has to be built into the presentation of a major research and development program right at the very beginning of things where authority and money to support such a program are under consideration. To emphasize classification guidance when you are working on a Development Concept Paper is getting off on the right foot. Furthermore, the guidance when written out has to be approved, in its technical characteristics, by the Director of Defense Research and Engineering himself. This is something very important, because, knowing as we all do now the attitude of Dr. Foster on making classification guidance in research and development a real, living, and practical thing, we know what we have to live up to if we're going to get his approval on guidance of technical characteristics in these major research and development programs.

There are other programs in research and development that don't require a Development Concept Paper, but are extremely important in the military services. And here, too, it is now a matter of policy that whoever prepares the program guide for a major program has got to get the approval of the guide at the level of the Assistant Secretary for Research and Development, or his designee. That raises the importance of guidance right to the top and will inspire everybody to do the best possible job he can, both on a timely basis and on a quality basis. And so these pronouncements reflect the attitude of the top echelon of DoD that classification guidance of real quality is a must, is a way of life from day to day now.

But more than that, beyond this development in classification guidance, it was announced by the Deputy Secretary of Defense that when we come to making classification determinations or declassification determinations, there

is a very important new element added as a matter of policy. This is an element of weighing advantages against disadvantages to the United States that would flow from classification as compared with open public release. This element applies where we determine that a U.S. lead time advantage is indispensable to the interests of national defense. If that determination is made, we must then evaluate our own national level of technical competence in the area involved. There is considerable support for the idea that the U.S. enjoys a degree of worldwide superiority in technological competence in a number of fields. If that concept is true as a general proposition, and if we determine that in a particular area we do have that national superiority, then, under the new policy, we must determine whether we can get the indispensable national lead time in an open race with other nations. If we can, then the policy requires that we won't use security classification. If we can actually make this policy concept work in practice, then the restraint of security classification in a very important program is avoided right from the start. And, of course, the absence of that restraint is likely to generate the greater emphasis and greater interest which will reach objectives a lot faster than would occur otherwise. That's a very important principle, and it means that if you find that that kind of worldwide superior technological expertise is ours in the particular area, then the information involved will be eligible for approval for general public release much sooner than if the classification/declassification cycle had to be observed.

Another pronouncement that was made at the level of the Deputy Secretary of Defense is that when you are writing a classification guide, you must identify milestones to force review for possible downgrading and declassification. Now, we have always had that policy objective. We've always said, as a matter of policy, that you must look at the situation critically and review it. But now it has been anchored for research and development purposes to the milestone concept. You might say there is a milestone at basic research, although there is very little classification at basic research. There's a milestone for advanced research. There's another one for development, another for production, another for deployment, and finally one for obsolescence. So now these things must be done. If they had been done over the years, we wouldn't have the mountain of classified information that we have to deal with now.

Finally, there were two other significant events that I want to mention. One was that Dr. Foster said to all of his principal staff assistants, "I want you gentlemen to develop classification guidance in specific technology areas starting with rocket propulsion and materials technologies." That was a brand new idea. It is very important because it means that if you do get these DoD guides in technologies, then, every program guide involving those technologies must incorporate the applicable parts of the DoD guidance in it. You will readily see that consistency in guidance will be more likely to be achieved among all of the various programs which involve those technologies. With this active direction and leadership from the Director of Defense Research and Engineering, we can expect to get some prompt and very capable input from his office.

The second event is that the Deputy Secretary of Defense issued a directive for cutting down on special access programs of every kind, with certain exceptions, in the research and development field. Accordingly, in August, and again in December, the Assistant Secretary of Defense for Administration went out to the services and other elements and said to them: "Come on in and tell us what you have in special access programs. For those that you want to continue, justify them. For those that you can't justify, cut them off." And so, in part thanks to you, the Society, because you, through your officers and directors, sent Joe Liebling a letter on this subject which he was able to use, along with

certain other letters, in advocating at top level this elimination of special access programs. All right. Have we achieved it yet? No. But I can assure you that we are still working on it and that it will be achieved.

Now, on every occasion when Joe Liebling has appeared before you, or before other audiences, he has said that downgrading and declassification are an absolute must. He said so here this morning.

If you people could know what we've been learning recently about the mountain of still surviving classified information that is around, I know you would realize that something is wrong with our system. Either we are classifying too much, or not downgrading and declassifying enough, or a combination of both.

And so, I really think that it's appropriate to emphasize that those people who have the responsibility at a command or supervisory level for the verification of classification determinations should really begin to apply a greater amount of their own personal time and effort in assuring that these determinations are necessary and are correct. And I think that they should also be willing to say, if they can't find sufficient support for a classification determination, that you will knock it off; you will not classify.

You know, for years and years it's been said, "If in doubt, classify." That's old hat! Nowadays you should be saying, "If in doubt, find out."

Commanders and supervisors are by directive responsible for reviewing and approving classification determinations made under their jurisdiction. And I hope that somehow the time has come when we can encourage these people to use that authority much more emphatically than they have in the past.

It is common in the field and some other places to hear it said how good it would be to see the general in person and to have a little heart-to-heart talk with him. If the general does let you know that he is aware of your presence by occasionally saying, for example, that you have made a mistake, or that you haven't shown a justification for your classification, then I am sure you would conclude that he is interested in your doing your classification job right. If such experiences took place, I'm sure you'd be motivated to do a better job. So, we are trying to establish this command level interest and action in the areas where original classification determinations are made.

On the other side, there are those of us who follow the decisions made by somebody else, the so-called derivative classification. You know, the guidance that is issued and comes to us can be applied with care or with indifference. Unhappily, I have a sneaking suspicion that a lot of people don't even want to know whether there is guidance available or don't care whether it is available. This state of mind can be found at the level of the working man who is writing a paper or working on a production line. We have to, somehow, bring it to the attention of these people at that level that there is guidance available and that they have the responsibility to apply it and make it work.

I think we are making progress in this connection. For example, in the development of guidance, when people come together and talk about it, they have in mind what the fellow at the working end is going to think about the guidance when he gets it. There is one particular area where this kind of cooperative effort in preparing good guidance is paying off. That is in Safeguard. Safeguard has been around now for several years. The Safeguard Classification Committee meets periodically. They see to it that the guidance for Safeguard is correct and is kept current. Right from the very beginning, this guidance has been worked out in the camaraderie of people from AEC and DoD and elements of industry, and they are thinking of the working guy so that he can understand it and apply it. This is

an example. All of you, and all of us, in all programs should see to it that the guidance gets down there and the people read it and make it work.

At this Seminar, I hope you will hear some new ideas on how to achieve some of these approaches. I hope you will hear that education and training are high on the list of musts for you as they are for us. I hope you will hear new ways of how to achieve classification decisions, perhaps on a more centralized basis.

I want to refer now to a few examples of the things we've done this past year which I think are important. First of all, I want to refer again to rocket propulsion. Very soon after the Director of Defense Research and Engineering issued his directive to his staff, a DoD Instruction was published. It is DoD Instruction 5210.59. It was done in record time. It's out there and available to you. It says, in part, that everyone running a program guide will incorporate therein the appropriate portions of the DoD Instruction. An Instruction in materials technology is also on the way.

We also have published a DoD Instruction, 5210.58, giving classification guidance on Nuclear Electromagnetic Pulse. It has a classified appendix which may be obtained on a need to know basis.

In the field of airborne radar, we have a DoD Instruction, 5210.57, which provides classification guidance at the DoD level. Recently, after a very long effort, we succeeded in establishing the DoD policy that airborne radar imagery of potential military targets will not be classified on the single ground that such imagery may provide a degree of targetting assistance to a potential enemy. This accomplishment means that people who operate airborne radar systems will not, for the most part, need to worry about whether a radar picture of a place on the ground has to be classified initially, unless, of course, the place is within an area contained in the so-called Consolidated Classified List, in which case, initial classification is required pending review by DoD.

We are working very hard in the field of lasers. The AEC and DoD are working closely in this regard. It's a rapidly moving field. There's a lot of impetus to try to keep laser technology unclassified. We have some DoD guidance out now that is up for revision. I'm sure that we're going to make some real progress.

It is in the area of DD Form 254s where most of you people from industry come to grips with the classification guidance problem. Here, we have achieved some results on proposed policy changes. The solution of the service contract problem is, I think, going to be that there will no longer be any requirement for a sign off by a government official on a DD Form 254 for such a contract. However, a DD Form 254 will be required to be used to give notice of the letting of a classified service contract. Also, there will be an option built in so that the government may use DD Form 254 for other purposes in connection with administering that kind of contract. We've also reached a point where I think we are going to eliminate the requirement for a government sign off on a notice of no change in classification guidance. You brought this up at the Seminar last year, and I'm sure it's close to solution. With respect to the idea of delegating authority for government sign off on a DD Form 254 for a subcontract, I think it will be possible to provide that that authority may be delegated to any contract administration office that's close to the place of performance of that subcontract. I think you want these things, and we're working toward trying to bring them about in accordance with their merits.

I am not going to mention any more specific accomplishments. I do want to say, however, that the Army, the Navy and the Air Force have been very busy during this past year in actually promoting and achieving some Classification Management objectives. There's been a lot of activity in the field of

downgrading and declassification. There's been a lot of activity in education and training. There's been a lot of activity in helping people who request elimination of classified elements from voluminous and frequent reports so as to make them easier to handle.

With that, I am going to conclude because my time has run out. I am so glad that you're here. We want you to go away from this place believing that this Seminar has been very worthwhile and has given you many new concepts and ideas on how to achieve Classification Management objectives in government and industry. Thanks very much.

Remarks of Colonel George A. Zacharias, USA —

Support of the Classification Management Program by the Office of Industrial Security rests in the hands of our Classification Management Specialists. Each Defense Contract Administration Services Region (DCASR) has a full-time CM Staff Specialist. He is the backup man in the effort to assure that contractors are provided meaningful classification guidance through all stages of a classified procurement. We recognize that the Government has agreed to furnish precise classification guidance for each classified bid, proposal, quote and contract; and, to issue revised guidance at any change which warrants downgrading, declassification or even upgrading. The basic responsibility for such actions lies with the Government procurement activity. Accordingly, the classification specifications you receive with each classified solicitation or contract identify the person and office where inquiries can be referred. Unfortunately the designated office may be far away and communications are sometimes delayed. We know also that the opportunity for an on-site discussion of a classification problem directly with the Government project man in the technical office concerned is sometimes difficult to arrange. On the other hand, a Government man that you see much of (possibly some of you are thinking that you see too much of him) is the Industrial Security Representative. The IS Representative is the eyes and ears for the Region CM Specialist. By the terms of our operating manual (revised since your seminar last year) the IS Rep is required to seek out and report classification problems to his staff specialist.

That same operating manual charges that the CM staff specialist is the focal point for coordination, assistance and advice to the IS Rep, the contractor and the contracting officer on classification management matters. I am pleased to report that there have been several coordinated successes since I addressed you last year. In a couple of cases, a cost savings was clearly indicated.

Example #1: There is regularly the question of assembly, component, or piece part classification when the end item hardware is classified. Too often subcontract 254s call for piece part classification just because the prime end-item is "known" to be classified. One of our East coast contractors who was engaged to manufacture "windows, for the outer flash assembly" was unsuccessful in explaining to a procurement activity that the "window" was being manufactured for several contractors and most procurements were unclassified. So as a matter of security interest the entire situation was explained to his DCASR IS Rep. The Rep saw the conflict, and possible overclassification, so the matter was summarized and turned over to our CM Specialist. The CM Specialist furnished all the details, through the proper procurement channels and arranged for a meeting between a service technical representative, the contractors involved and the DCASR Industrial Security Representatives. This coordinated effort resulted in adequate and productive classification guidance and piece part procurements are handled on an unclassified basis. This is a simple example of what can be done; and, although we didn't measure just how much, there are now savings in

security costs being enjoyed by the Government and the contractor who mentioned the case on one of his routine inspections.

Example #2: In another case involving component classification, the combined efforts of a California contractor and DCASR, San Francisco brought about a declassification action which resulted in a cost savings of $20 per unit. To date there have been 660 units manufactured since the declassification action. In terms of big business $13,200 doesn't sound like very much but consider what savings would amount to if we could effect a savings of $20 per unit on one component in every 254 being used today.

Example #3: A meeting was arranged by the Office of Industrial Security, New York between the Security Manager of a large northeast contractor and the AFPR and his Chief Contract Administrator.

The contractor stated they were awarded a contract and the entire document including the General Provisions (ASPR Clauses) and the DD Form 254 were classified confidential. To perform on this contract approximately 100 subcontractors would be solicited.

Our Classification Management Specialist returned the contract document to the Procurement Activity requesting a security classification review in line with DoD Instruction 5210.47, Security Classification of Official Information, Paragraph VI-B, Identification of Information Requiring Protection.

In response a revised DD Form 254 was issued declassifying all portions of the procurement document which did not contain sensitive information. This action permitted the contractor to proceed to subcontract on an unclassified basis.

Taking a raw figure of $250 as the cost for processing a Facility Security Clearance, it is estimated that cost avoidance, by the intervention of our office, prevented an unnecessary expenditure of $25,000.

Effective classification management is necessarily a team effort. The DCASR CM Specialists are in regular contact with some classification managers of the User Agencies. This week will not be an exception; to take full advantage of this event I used some persuasion with the Region Commanders to have their CM Specialists arrive by 8:30 Monday morning. We also prevailed on several contract administrators and classification managers from the major User Agencies with headquarters in the National Capitol area to join us in an all-Government workshop. There was one agenda item: "A free exchange of ideas, problems and solutions for the betterment of the Classification Management Program as it is applied in the Defense Industrial Security Program." The day-long discussion was geared to the single purpose of finding additional ways whereby security classification practices and procedures can be improved for the benefit of all concerned. The free exchange got really swinging at times but no one was really hurt and the results will be productive in the months ahead. (On behalf of all the Government types who participated Monday I wish to thank your Society for making conference space available for us.)

A moment ago I mentioned a team effort. Actually the team I reference is a three-party team. I am told that most of you are security classification managers for your respective companies. You and others who do the CM job in industry are the third party on the team. Actually you are the team captain because your interests and actions get things done. As you know, the Defense Industrial Security Program does not, in so many words require that contractors have staff security classification managers but there has been a long-standing policy of the DoD to solicit contractors advice and assistance in classification management matters. Further, you are called upon to establish procedures to insure that a determination of necessity, currency and accuracy of a classification is made before it is applied to a document (paragraph 10, ISM). Also, we hear that there

are many contractors suffering with out-moded classification guidance. Yet over the years very few cases have been documented and submitted. Of the few cases referred for reconsideration most have resulted in changes favoring the contractor's point of view. The ASIS Classification Management Committee estimated that 80 percent of the nation's classified material is in the hands of industry, therefore, effective classification management calls for a continuing evaluation by all hands. The optimum is to have necessary protection while simultaneously promoting downgrading and declassification. As security classification managers you can help us (Government) add strength to the Classification Management Program.

With the splendid cooperation of some classification-minded managers in industry, the DCASRs have carried the cross many times in the past year and have gained satisfying success. We have redefined and broadened the CM Specialist's mission; similarly we have given new direction to the Industrial Security Representatives by reorienting the importance of their role in the field of classification management. A currently dated DD Form 254 is no longer the only interest; they are instructed to determine that the guidance is adequate for contract performance; that it is accurate and consistent with other known classification state-of-the-art. All we ask of you is to discuss your classification problems with us.

* * * * *

U.S. CONTROL OF NON-CLASSIFIED INFORMATION AND COMMODITIES
BY
HUGH P. DONAGHUE

When I looked at your program, I thought I'd discuss with you a topic that I call the gray area of United States control of non-classified information and commodities. It is an area that needs further understanding on the part of both industry and the government.

What I want to do is give you a couple examples of the types of controls that sometimes industry finds are applied to products that come out of our own research and development. This involves products in both the commercial area and in some areas on the military side. These products are developed using our company's own research and development dollars, and are high technology items.

The regulations that sometimes govern and control our activities in this area are such things as the Administration's Export Control Act of 1969, the United States Munitions Control List that we live with; and other regulations, things such as Truth in Negotiations which in many instances posed a serious dilemma to us in industry.

The first case I would like to cite goes back to 1966 when Control Data was producing a machine which we called the CDC-6600. We considered this machine to be the most powerful computer in the market at that time. We insist that we developed that machine on our own research dollars.

In 1966 Control Data was having serious problems with the United States Government over the issue of Truth in Negotiations. At the same time, we found that we had an inability to sell these machines overseas, where there seemed to be a rising and growing market. We were particularly having some very strong difficulties selling to the French because of an embargo on any of our large computers to the French Government.

The basic reasons for the U.S. decision on this particular machine were solid and were valid. France was a non-signatory to the Test Ban Treaty, and two of the applications that we had pending at that time were for the French Atomic Energy Commission.

On the other hand, we had several other computers for French industry —

for the French Electric Power Company; for a service bureau — and all these systems were held pending an agreement that at that time had not been established between the French and the U.S. Governments.

In spite of many pressures by our company on the U.S. Government, we just had to wait out this time period until an agreement was established in September of 1966 which allowed for the sale of machines such as the CDC-6600 to France but excluded sales to the Weapons Laboratory.

While we were facing this particular problem, we were facing a problem at home with our own Atomic Energy Commission involving the Truth in Negotiations Act.

Because the U.S. Government was the prime purchaser of our machines at that time, they insisted that we should be giving them all cost data that we could possibly give them on the 6600 so that they could realize whether or not they were getting a good deal.

The reason though that the Government was the largest purchaser of our equipment at that point in time was simply that they wouldn't allow us to sell elsewhere to establish a market. In one of my discussions over this Negotiations Act with people in the Government Services Administration who were acting as a spokesman for the Atomic Energy Commission — and they were about to testify before the Proxmire Committee — they approached IBM and Control Data as to our willingness to provide these cost data, prior to their going before the Proxmire Committee. Their approach to me was that everybody else had said they would be willing to give information on machines such as the CDC-6600 and the comparable IBM version except Control Data and IBM.

This was the situation that we were facing at that time; the only two manufacturers who had machines that the AEC desired at that time were those two manufacturers. All others would be willing to give their cost data if they indeed had a machine that would be affected by it.

More recently, we had a case involving the Soviet Union. This was a very interesting one.

Back in the last part of 1968, a visit was made to a research institute called Serpukhov in the Soviet Union by some members of the U.S. Atomic Energy Commission. Serpukhov had at that time the largest — or still has for that matter — the largest linear accelerator, 76 million electron volt accelerator. Our scientists were interested in obtaining some of the data that came from that accelerator while we were waiting for our own to be built.

The Soviets said, well, that's not a bad idea; we wouldn't mind sharing it with you, but we just can't see the logic in sharing this data with you when you can process it with those very powerful machines that you have back in the United States. What we would like in return for giving you this data is for you to allow us to have CDC-6600.

The scientists came back and it was argued within the realm of the government for many many months, and it was then determined that it wasn't in the best interest of the United States Government to allow this to occur.

As soon as this decision was made on the part of the United States Government, the British stepped in. And they offered a new system of their own whose power would be just approximately equal to a single 6600. And again, the powers of the U.S. Government, because there were United States verbals attached to that computer, decided it wasn't still in the best interest of the United States Government to go along with this. So the British were informed that no U.S. approval would be given.

Prime Minister Heath when he was over here last December made an overture to the President that he felt the case needed reconsideration. The case was reconsidered and as of two weeks ago,

the British were informed that their two machines could be sold to the Soviet Union to do the same processing that Control Data were denied not more than a year ago. When I attempted to inquire as to how this could be in our free enterprise system, I was informed that U.S. industry unfortunately doesn't have an ambassador, and Mr. Heath constantly pays visits on behalf of their industry.

One last point I would like to cite as an example is the dilemma we face with small computers that fall under the process of munitions control.

From time to time Control Data, like other manufacturers, decide that areas such as small avionic computers are areas in which we should invest our R&D dollars.

Unlike the standard product, when it comes to items that fall in the Munitions Control List — and these do — we are required to go to the government for permission to even submit a proposal to a foreign government or to a foreign firm. Quite recently, we have come out with a fairly new, again very high technology, machine on which we have submitted several proposals for incorporation both in some of our own weapons systems here in the United States in addition to those overseas.

Again we understand fully the game we're playing. We certainly would like to sell most of these computers to the United States Government and to the military forces that have taken them under evaluation. But the dilemma we find ourselves again facing us, is one where the government will purchase one of a kind for evaluation purposes. Then you're in the position of being denied the ability to talk about that machine or to propose that machine in other systems.

As a matter of fact, in one recent denial that we had, we got a very nice commendation that said: The Department of Defense had commented to the effect that this particular computer is to be used in several classified weapon systems by the U.S. Navy and has potential use for others, including strategic weapons. The computer is considered to be a major advance in many computer designs. It has great potential for DoD's weapon systems. The DoD consequently desires that requests for the export of this computer be denied until research and development on the system has been completed and the planned weapon users of the computer are more definitively known.

Just recently, I cameback from a trip to Europe to find that we lost two out of the three proposals that we had in to the government. The loss might have been in dollars; it might have been in performance. Meanwhile, the business overseas has also gone by the board.

As to this particular machine, we were actually talking to a firm in West Germany who not only wanted to buy the computer for use in a NATO weapons system but also was interested in the manufacturing rights of that machine. To give you an idea what that means, Control Data would have to sell $18 million worth of those computers here in the United States to reach the same net profit as the transfer of that manufacturing license alone to West Germany. That's quite a few dollars in sales.

This type of dilemma is the type that we in industry constantly face. Different regulations, all logical and justifiable in their own right, would seem to counteract our ability to either do business here or do business abroad. Some of these days, I keep saying, the government and industry are going to have to face up to this.

* * * * *

SECURITY CLASSIFICATION MANAGEMENT AS PRACTICED BY OTHER GOVERNMENTS

BY

S. M. JENKYNS

I would be remiss if I failed at the outset to acknowledge the leadership

of your government and industry in this very effective discharge of the responsibilities of security classification management.

I don't wish to break my arm patting you all collectively on the backs, but the results of your labor are evident in their acceptance beyond the continental limits of the United States, in NATO and in other bilateral arrangements such as we in Canada enjoy with the United States.

My own personal experience in working with the Office of the Chief of Industrial Security, Colonel George Zacharias and his predecessors and their staffs, and other members of the Department of Defense has been a very rewarding one for myself personally; and we in Canada owe a lot to persons such as are employed in your government and industry.

To understand Canadian security classification management perhaps I might just take a few moments to make you aware of certain changes that have occurred in the past few years.

George MacClain mentioned the Department of Defence Production. It is the predecessor of the present Department of Supply and Services. At the end of World War II, we did have the Department of Munitions and Supply which did the purchasing for defence equipment in Canada. We also had a unit known as Canadian Commercial Corporation, which in fact still exists, but in 1951 the government organized the Department of Defence Production, which included CCC.

It was in September 1963 that the Department of Defence Production was altered to make it the focal purchasing point for all departments of government. This was the result of one of the Royal Commissions known commonly as the Glasgow Commission of 1962. At that time, the Canadian Government recognized the need to incorporate not only defence procurement but procurement for the civil side of the government.

In July 1968, the Prime Minister announced the emergence of the Department of Supply and Services as a result of a total reorganization of government departments at that time, and DSS incorporated units from areas such as the Comptroller of the Treasury, the Public Service Commission, the Bureau of Management and Consulting Services, and so on.

The unit for industrial security, however, did not alter basically from its inception following World War II. It had originally been the responsibility of the Department of National Defence, but due to changes in organization within DND, it was decided after a study had been made that industrial security should be under the contracting authority and it was then transferred to Canadian Commercial Corporation. This, as I mentioned earlier, was eventually gobbled up by DSS, and so the industrial security side of the house remains now in the Department of Supply and Services.

The cycle of equipment programming which has four parts in Canada, two of which are decision making and two of which are decision implementing, can be identified first the recognition of the requirement, second the definition of the equipment to meet the requirement, third its funding, and fourth procurement.

It's almost impossible to stress too strongly that the aim of capital equipment programs in the armed forces is to satisfy the operation in those forces. The two lead off documents for equipment proposals echo this. They are Operational Equipment Objectives, which state the need and Operational Equipment Requirements.

As you know, the user department is the Department of National Defence and this department expresses its need in the original OEO. Earlier this morning one of the speakers mentioned the need for incorporating in the Operational Equipment Objectives the security requirements of the work. This is usual in any major weapons system or equipment family, and is the basis for engineering and technical studies to determine what is feasible.

Then an Operation Equipment Requirement is prepared which is again the user responsibility (which is the Department of National Defence) and coordinated within Canadian Forces Headquarters. This OER sets out the performance characteristics of the equipment, its physical specifications, maintenance requirements, organization, manning and training implications, and compatibility with other equipment, and so on. It also incorporates at that stage the security requirements of the work.

The OER having defined the piece of equipment to fill the need for a feasible Operation Equipment Objective is examined by the Chief of the Technical Services Branch of the Department of National Defence. He considers — or that branch considers — all the contenders available to supply the equipment and how they appear to match the OER and what they cost.

When there is nothing on the shelf to fill the bill, then a research and development project may be recommended which might well be tied in with other departments of government, other parties to military standardization agreements with Canada, and with Canadian industry.

When interdepartmental coordination may be required, the Department of National Defence, representing the user, prepares a Program Change Proposal, which is the vehicle by which the stated requirement will be carried to success through the Treasury Board's submission, and sets the specifications for possible contract.

When the Program Change Proposal has gone the rounds, it is presented to a Program Review Board where it is programmed into the defence budget for capital equipment.

During all its process through the various DND in-house steps, interdepartmental coordination and Treasury Board approval, the submission is subject to continuous review for need, priority, availability, better alternatives, conflicting commitments, and new policy decisions.

Upon final Treasury Board approval, the sequence of raising a contract demand by the Department of National Defence — the putting out of request for tenders, drawing up contract data, reviewing tenders and security contract approval by the Department of Supply and Services — is common to most government procurement.

By now, you will have recognized that there are some slight differences between our procurement cycle and yours in the States. Where you have contracts let by the individual departments of the Army, Air Force, and Navy which are then monitored by the Defense Supply Agency, Canadian defence contracts are let by the Department of Supply and Services and industrial security becomes an integral part of the contract process from the outset, with responsibility through the pre-contract, contract, and post-contract stages.

The continuity of the security requirements from the outset is provided through the Department of National Defence, Directorate of Security, which is included in the group which establishes the Security Requirements Check List — or as you refer to it in the States, your DD 254.

The Directorate of Security in turn through the research and development phases reviews the classification requirements every six months. Both reviews — that which is conducted six-monthly in the R&D and an annual review made by the Department of National Defence in the production phase — are coordinated with the Industrial Security Branch of DSS.

I should mention also that the Department of National Defence has its own Defence Research Board, with its own security office. This office performs essentially the same functions as the Directorate of Security. It coordinates with the Directorate of Security and our branch when required for industrial participation, and, again, their contracts (DRB) are let by the Department of Supply and Services.

I would be remiss if I didn't confuse you further by referring to other R&D programs which are initiated by yet another department within the Canadian Government. These are programs that are initiated in Canadian industry through the Department of Industry, Trade, and Commerce, which may embody from time to time U.S. programs of industrial research and development.

First is the Industrial Research and Development Program generally which is designed to provide for the payment of grants based on expenditures for scientific research and development carried out in Canada. Industry, Trade, and Commerce have been watching the research programs carried out by major nations of the world and recognize that Canada has a deficiency here because it is difficult for small companies to compete with large companies in conducting this kind of research. Programs are partly financed at times on a shared basis with other governments such as the United States, on a selected basis, however, to avoid costly duplication of time, effort, and money.

There are other programs of research and development particularly aimed at the commercial side: PAIT, Program for Advancement of Industrial Technology; IDAP, Industrial Design and Assistance Program; and we even have one called PEP, Pep Program. The objective is, of course, to induce improved productivity in all manufacturing and processing sectors in Canadian industry.

While the last three of these IT&C programs are primarily designed for the commercial side of industry, the first often includes defence information. When it does, the Industry, Trade, and Commerce Branch responsible is the International Defence Programs Branch. This used to be the International Programs Branch of our old Department of Defence Production.

On transfer to the Industry, Trade, and Commerce Department, responsibility for industrial security on their behalf has remained with Industrial Security of Department of Supply and Services. This has included membership in working parties of Canadian and U.S. such as with the U.S. Department of Defense.

All government information in Canada, which naturally includes defence, is classified for security purposes into four categories; and they correspond, three of them, with yours: Top Secret, Secret, Confidential; and we add Restricted, which is information which should not be published or communicated to anyone except for official purposes.

There are slight differences in terminology. Our definition of Top Secret is similar to yours. It is "information the unathorized disclosure of which would cause exceptionally grave damage to the nation." Secret — "the unauthorized disclosure of which would cause serious injury to the interests or prestige of the nation or any government activity thereof, or would be of great advantage to a foreign nation." I think you say serious "damage" to the interests or prestige of the nation, or any government activity thereof which would give great advantage to a foreign nation.

In Confidential, we have added a little bit more to yours: "the unauthorized disclosure of which while not endangering the national security, would be prejudicial to the interests or prestige of the nation." And we have added: "any Canadian activity or individual or would cause administrative embarrassment or difficulty or be of advantage to a foreign nation."

We have similar regulations to your own for the protection of classified documents, their marking, whether bound or not bound; whether material is concerned and how it's marked and so on. These are all regulated in similar manual form such as your Industrial Security Manual and other manuals in government use.

As I explained earlier, defence information which is initially classified by the Department of National Defence is classified according to

these categories and certain precedents which have been established. They take into account state of the art, intelligence, security input, and these are provided at the inception of the programs. But specific classifying criteria, as you have, are not spelled out. We have an advantage too perhaps over you in that we are able to control the security classifications at the headquarters level. There is no need, because of our smaller size, to have classifications assigned at Commands or lower echelons.

One distinction that we have made since the earlier days of our classification program has been to accord somewhat higher classifications to the R&D programs over production programs, since we recognized early that these are the programs where it is necessary to protect lead time and must be of a higher classification than production or field use classifications. However, it would appear that the Canadian process has been rather a hit or miss effort in this regard, which has fortunately had certain inherent characteristics which, without formal recognition, have actually met what are now accepted as criteria for classifying defence information.

I may perhaps be pardoned for making such a statement since this occurred when I was head of the RCAF Intelligence-Security Section and Secretary of the Joint Security Committee of National Defence, when my office initiated with the other two service intelligence units a review of the security classifications assigned to various defence projects. At that time the RCAF was engaged in the design, development and production of its first all-weather fighter, CF-100 (Canuck). I regret to say that since that date we seem to have done little to formalize criteria except design an SRCL, a Security Requirements Check List, to improve the situation.

The method of identifying the security classification level to all users in Canada is through this Security Requirements Check List. It's similar to your DD-254. The practice which we have followed in recent years is to request industry to comment on the acceptability of the SRCL prior to formal acceptance. Following six-monthly or annual reviews, amendments to the classification levels are circulated as amended SRCLs to all users.

Canada does not have a time-phased automatic downgrading declassification program. We rely instead on the six-monthly and annual reviews and the smaller, comparatively speaking, number of classified programs in force at any one time.

I suppose we have one problem which is universal to yours and other NATO countries, related to the actual disposal of classified documents in industry when the information has been formally declassified by government.

Instead of welcoming the release from security restrictions on lockups and document handling, some industries tend to retain as much material as they can in their record libraries, unfortunately without benefit of formal declassification action. We have instituted a program of inspection and document disposal review in Canadian industry which we hope in due course will pay dividends. It was interesting to hear the speaker this morning mention the reduction in cost possibilities. Should we get proportionately a return of as much, I'm sure we'll be very happy. [Reference to General Coffin's presentation.]

On the other hand, we have found at times our Department of National Defence rejects initial attempts by industry to downgrade or declassify technical project reports. The first reaction usually is that current SRCLs do not require amendment; and this is quite possible. They feel that reports should continue to retain the classification level, however. Such insistence is often viewed with astonishment and disappointment by the technical experts involved in the projects who are knowledgeable of more recent developments and sophis-

tication.

Among the factors about which we are vitally concerned is the attempt to employ security controls in impractical situations. Although we do not always advocate removal of security classification in such cases, we are very conscious of the possibility that such retention may degrade the classification system. In such circumstances a review will be made to determine whether the end purpose would be served in retaining a selected classification level.

Originators of security classification are aware of the need for review when unofficial publication of information on a classified project appears, although they are warned against confirming such publication without benefit of the classification review. Should such review be made and confirmation ultimately result, an amendment to the SRCL would be issued and circulated.

Well, you have your Pentagon Papers and we had our Spencer case and the resulting Royal Commission on Security. Our Royal Commission on Security published its report in June 1969. Where classification management played a big part in your case, the only mention of security classification management appearing in the Royal Commission on security's report concerned the industrial use of the SRCL. The Commission recognized, and I quote:

"That proper classification of the various aspects of the classified contract were of considerable importance to the effective operation of the industrial security system for over-classification or unnecessary classification can place a considerable burden on industry."

The Commission also stated, and I again quote:

"The need for classification should be balanced against the cost and effort required to supplement the necessary procedures. The need to declassify a specific aspect of a contract as the contract proceeds should also be considered; and consultation with industry should exist."

Without wishing to appear critical, since the Royal Commission on Security had a lot of ground to cover and security classification management was only a small part of the overall entirety, as a security specialist I feel this observation was very limited in its scope. I feel naturally that to be properly effective, security classification management must start at the cradle and end at the grave, not somewhere in between.

I agree, however, that where industry is involved they should have a say in the protective requirements, or rather the method by which protection can be provided, particularly when classified information is in the contract process. I firmly believe that Canadian industry has a great deal to offer, as does United States industry in your country.

Our job in industrial security at DSS is to act as an intermediary in such areas, and we are finding more and more that review of security levels on a periodic basis is paying dividends. Not only is the program review necessary, we also feel that reviews are required as events occur, and the periodic six-monthly and annual reviews. A combination of all will be the most rewarding.

I'd like to refer to one of the newer problems — or problems of recent years — that of computer security — and only briefly.

One of the basis for providing security classification to R&D programming was and no doubt will continue to be for the purpose of protecting lead time. This was also mentioned this morning. It would be incongruous then if security classification management did not take firm steps to relate their objectives to the use of this new tool, the computer.

In Canada few if any of our SRCLs contain provision for protective requirements for the use of computers in government and industrial work.

The accent has been to provide security guidance to those ADP/EDP firms who are working exclusively on computer type contractual requirements. Here it is easy to define a "dedicated computer" operation and to restrict certain areas where "shared time" and "remote-mode" operations are involved. Unfortunately, we find we are leaving some firms to make their own decisions on the use of somebody else's computer facility to speed up certain technical data processes.

The degree of protection particularly in this realistic atmosphere, in this age of computers, where the lead time in R&D work may be adversely affected, at times without knowledge, presents a great challenge to a society such as yours. I am pleased to see from your society's brochure that you recognize the problem, and I refer to one of your Seminars on Classification Management in the Computer Environment. I think this is really great.

To provide security classification management on a realistic basis in the R&D environment and through the life cycle of a classified project with the attendant inroads in split time operations of the computer age will indeed test all the ingenuity of the security classification management specialists.

In summary, therefore, Canadian defence security classification management is initiated by the Department of National Defence at the headquarters level, using government classifications — Top Secret, Secret, Confidential, and Restricted, similar to yours in the United States with the exception of Restricted. This is done in conjunction with the Directorate of Security at headquarters. Where contracting with industry is concerned, Industrial Security, DSS, is advised and consulted. A joint group establishes the security classification levels.

We do use practical precedents, however, rather than formal criteria to establish these security classification levels, but it's hoped through attendance and participation in seminars such as yours that more formality will result. We do, however, review from time-to-time criteria which are used by other countries such as your own, and we find that we do use similar criteria but they're not set out in the form that you use.

All users of defence information so classified, including the contracting authority, Department of Supply and Services and industry, are made aware of security classifications through the medium of SRCLs — Security Requirements Check List. Changes in the security classifications are circulated to the users by amended SRCLs as required.

We do not have an automatic time phase downgrading declassification program. We do use yours when we do contracting, however, involving information of U.S. defense origin under U.S.-Canada Industrial Security Agreement procedures.

We review on a six-monthly basis the research and development phases and on a yearly basis in the production phase, unless some change has occurred in the interim. In this regard, we benefit greatly from our smaller number of classified defence projects which enables us to do this on a case-by-case basis. I hesitate to think what we would do if we had to face such a problem as mentioned this morning by General Coffin. The number of scientific papers and authorities that must be gone through here — it's tremendous.

The monitoring of security classification and our amendments are regulated throughout government departments and industry. All monitoring of industrial security classification management, including acting as intermediary with the originators of security classifications, is performed by Industrial Security of DSS but the final determination rests with the Directorate of Security and the project officers of the Department of National Defence.

We have recognized the need for more detailed study of the new threat to our security classification program such as brought about by the use of computers. In this regard, Industrial Security has taken the lead in initiating a total government review of the problem.

We welcome inspections by NATO and your government on the security arrangements under our bilateral agreements. We trust you on this. More importantly, we welcome the opportunity of working with our U.S. colleagues in government and industry.

Questions and Answers —

Mr. Bagley (Naval Research Lab.): Do you have an Official Secret Act in Canada analogous to that in Britain?

Mr. Jenkyns: Yes, we do. It's called the Official Secret Act.

Dr. Klein (Army Night Vision Lab.): I'd like to know what constitutes the 6-month review that you use instead of the automatic downgrading. In other words, do people at the working level have to report how much they have downgraded or give some kind of justification for holding the classification? How does that actually work?

Mr. Jenkyns: Well, the review is done at headquarters level. And then if it's in industry at all, it's done through the Department of Supply and Services and Industrial Security, much in the same way as your DSA [Defense Supply Agency] works in industry in the States. We ask for classification objectives, reviews, amendments in industry and this is put together at 6-month intervals.

Dr. Klein: But who makes the determination that a particular document may be downgraded?

Mr. Jenkyns: The Department of National Defence at the originating level, headquarters. There is no command specialist that controls security classification management. It's all done at the headquarters, centralized level.

Mr. MacClain: Have you any idea how rapidly your classified information becomes declassified through the 6-month reviews that you give it? I mean if you declassify information, then presumably you give notice of declassification. But I was wondering how rapidly from the time you start to classify a particular body of information that it will be determined that it no longer needs to be classified. Does it take any period of time, like years or months?

Mr. Jenkyns: No, the longest would be about three or four weeks. We have a much smaller group, remember. They are all housed in headquarters. They are called together at a moment's notice. They can be available by arrangement, by telephonic arrangement. And this is a review done by the project offices, the technical people, and the Directorate of Security of National Defence initially.

Mr. MacClain: Let us suppose you are going to develop a weapons system and it takes a few years to accomplish that. During the initial stages you probably classify some information and your program goes on for a few years. At what point in time — years from the starting point — do you begin to declassify information belonging to that program?

Mr. Jenkyns: Well, that's getting into the life cycle. That takes a lot longer. The first question that you're talking about, having made a determination to get together and review a classification, the time it takes to make a decision is relatively short. And the time in passing that decision on to the users is also short.

Over the life cycle of an R&D program, this 6-monthly review may occur several times. In the case where a change occurs in that 6-month period again the time required to tell the users and the holders is relatively short. At that point in time, we have probably fewer people involved in it

than you might expect. We are not a command-oriented type as you are.

Mr. Florence: In Canada is there any penalty for assigning unjustifiable classification?

Mr. Jenkyns: There is no such penalty.

Mr. Ritzel (General Electric): In your 6-month review, what has been the percent average of downgrading or declassification in this period over the years? In other words, when you make a total review at 6 months, do you usually downgrade or declassify 10 percent or 15 percent, or what do you normally average?

Mr. Jenkyns: In the R&D programs, it would be very little. We find there's a very small percentage downgraded in the 6-month review. But they still feel that this is necessary even though it is such a small percentage. It is not large. I don't have the precise figures, however.

* * * * *

IMPACT OF SECURITY CLASSIFICATION AND PATENT SECRECY ORDERS ON PROCESSING PATENT APPLICATIONS

Remarks by Edward J. Kelly —

The aim of this portion of the seminar is to review the impact of dual classification systems on the security management of patent applications. Since we are to discuss the applications coming under dual systems, we are limiting the coverage to the cases that contain classified information developed within the government and which, of course, come under Executive Order 10501 and the subsequent Executive Orders. It is clear that we are going to avoid those applications that contain privately developed and privately owned information and come within the purview of Patent Secrecy orders. Perhaps sometime in the future it might be possible to have someone give a presentation on the security management of these privately owned patent applications.

Since we are discussing information coming under Executive Orders that have as their title "Safeguarding the Defense of the United States," we are relating basically to Army, Navy, Air Force, DoD, NASA, AEC, and I shall call that group the "Defense family." This Defense family has throughout the years generated its own implementing procedure, which for the most part have deviated very little from the scope of the Executive Order.

It might be parenthetically mentioned that Executive Order 10501 contains two sections of interest from a management point of view. The first is Section 11 which states that: "The Attorney General . . . shall . . . upon request of the head of a department or agency or his representative render an interpretation of these regulations in connection with any problem arising out of their administration."

Second, Section 12 provides that: "Nothing in the order shall be construed to authorize the dissemination, handling or transmission of classified information contrary to the provisions of any statute."

Now, an observation of the Defense family implementations of the Executive Orders which might be called to your attention is a total absence of information that is peculiar to patent applications. Within the government agencies, the applications are treated the same as any other classified documents. When dealing with industry, procedural aspects are set out in the ASPR and the Industrial Security Manuals. They obliquely address themselves to the subject of inventions.

Thus, Section 9-106 of ASPR covers filing procedures for classified contractor filed cases; and the Industrial Security Manual, page 12, provides for the retention of classified material where it is patentable in-

formation and owned by the contractor. On page 50, direct transmittal to foreign governments is covered, while on page 53, reproduction authorization is set forth in connection with patent applications. This then, as we see it, is the defense security picture and the provisions applicable to classified patent applications.

Turning now to the Patent Secrecy Act; it was created to prevent the publishing of information in the form of a patent where such publication might be detrimental to national security. It was set up in spirit rather than definite procedural language, as is covered in the Defense Security Procedures. It should be pointed out — and I'm sure you all know — that the patent laws are statutes and that they provide generally for the publication and open dissemination of information as this is the meaning of the term "letters patent." There is a limited withholding of inventions while novelty is being ascertained but thereafter an individual is entitled to have his invention published. Since these provisions are statutory, the security regulations as set out in the Executive Order would be ineffective in the light of the limitations of Section 12, which I have mentioned earlier. Thus, it became necessary to provide statutory control of inventions if certain information, whose release would be detrimental to national security, was to be withheld from the open literature. Further, it was necessary to make these provisions statutory as they apply to private property as well as government property and they would impinge upon private rights. So the provisions that control inventions and patents are set up statutorily.

This is the purpose of the Patent Secrecy Act and the reason for its existence. It is administered in the main by the Commissioner of Patents on the advice of members of the Defense family. Mr. Campbell is Chief of the Patent Office Security Group.

Mention might be made here of an obvious question with an answer to it. Why does the government file and permit to be filed patent applications that relate to classified information? The answer is a simple one, namely, it is to the government's advantage to get statutory protection against claims of outside invertors who invent after the government's contribution; or to put it in other terms, the filing is undertaken to avoid claims in the procurement cycle that are based upon inventions made by the government and its contractors during the R&D cycle. Thus, filing reflects a balancing of two vectors that affect the defense mission — namely, security and infringement claims.

The President of the United States has expressed his policy on inventions in a statement to the Heads of Executive Departments in 1963 when he took official recognition of the fact that the government expends large sums of money on R&D and this results in a considerable number of inventions, and the inventions in scientific and technological fields resulting from this R&D work constitute a valuable national resource and should be prudently administered.

Returning now to the Patent Secrecy Act, some mention might be made of the provisions which affect classified applications. The entire Act is set forth in Sections 181-188 of Title 35 USC. The Act provides for a cooperative effort between the Commissioner of Patents and those agencies designated as "Defense Agencies." The group is currently limited to the Department of Defense, NASA, and AEC. Principal provisions provide that:

The Commissioner of Patents when notified by the interested agency shall order the invention to be kept secret — i.e., be controlled — and withhold the grant of a patent;

Upon proper showing by the head of a department or agency that the examination of the patent application might jeopardize the national interest, the Commissioner can maintain the application in a sealed condition — i.e., no one in the Patent Office may have access to it;

The Commissioner may rescind the order of secrecy upon notification by a member of the Defense family;

Application may be filed in certain foreign countries when so authorized by the interested members of the Defense family;

And there are provisions under which rules and regulations may be issued by the Secretary of Commerce or members of the Defense family.

Some comments on the foregoing: First, the actions by the Patent Office are initiated by the Defense family. Second, some cases, usually Top Secret or limited disclosure projects, may be filed without being examined and still get the benefit of the filing date. Third, cases may be filed in foreign countries — and today I think there are fourteen countries in which they can be filed. Fourth, rescission of the secrecy orders are initiated by the Defense family. And, finally, DoD, AEC, NASA may vitalize the provisions of the Act by rules and regulations.

Now with this background, I think it appropriate to outline some of the operational aspects of patent applications that contain classified information. I am now speaking as a patent attorney prosecuting government cases in the Patent Office. Mr. Waddell will speak from the point of view of a patent attorney in industry prosecuting classified cases in the Patent Office.

My particular organization is the Army Material Command. We file between 400 and 500 applications each year and we advance the prosecution of a total AMC pending case load of over 1300 cases. About one-fifth of these are classified. The classified cases bear the marking prescribed by Executive Order 10501 and are generally in conformance with the implementation regulations.

Our classified applications and amendments are delivered directly to the Security Group in the Patent Office. They do not go through the regular Patent Office channels. Each page bears a proper classification at the top and the bottom, as the application is not considered to be a physically bound document. The drawings are similarly marked.

Our cases are not placed under the Patent Secrecy Act during their active prosecution as their military classification as indicated by the marking afford them the same protection in the eyes of the Patent Office during the prosecution cycle. The reason for this delay is to forestall the use of the Secrecy Act until it is absolutely necessary, namely, when the prosecution has been terminated. At that time, the application will issue as a patent unless a Secrecy Order is applied to it.

This prosecution takes usually two to three years or more and provides an opportunity to have the classification status reviewed at the later completion date. If still classified at this time, the application is placed under the provisions of the Secrecy Act. It remains in this status until it has been determined that the subject matter is no longer classified, when it is then removed therefrom and the classification marks cancelled.

There are some areas in which the defense security provisions are unnecessary in that they serve no useful purpose and they have been avoided by the most circuitous reasoning or else honored in the breach.

The first area is that which contains the requirement that classified documents have paragraph classification, indicated by placing code letters at the beginning of each paragraph. This action serves no useful purpose in patent prosecution for nothing is extracted from an application that is filed as a classified case. When a case is placed in the Patent Office, it is a one-way street and it can only go out through the issue route, and will never pass through this exit until all classification marks have been removed. No one can extract any portions from it. All operations are

applied to it as a whole and it is processed as any other case coming under the Secrecy Act. From a practical point of view, the attorney who prepares the application develops a twenty-page document on the average from a two-page disclosure having classification markings on it. He has no picture of the different levels of classification that are applicable. Again, when he amends the case — and this goes on for a period of one or two years — you get an answer from the Patent Office and you reply back to the Patent Office — when he amends the case, he is at sea insofar as the individual paragraphs of his argument are concerned. Finally, when the case is ready to issue, there is a need for removing these markings and the one who does it is a member of Mr. Campbell's group in the Patent Office.

There are over fifty paragraphs in a patent application and it is very easy for somebody to overlook a C, an S, or a TS on a paragraph. So we think the action is unnecessary and it is conducive to errors. We think that corrective action is needed there.

A second area is the Automatic Time-Phased Downgrading and Declassification system. Executive Order 10964 provides for automatic changes in classification to the "fullest extent practicable" but no provisions are made for determining the practicability of such a program in connection with patent applications.

In the Patent Office, classified applications retain classification markings independent of periodic regrading. They remain that way until the attorney on the case notifies the Patent Office to cancel the classification markings. The requirement could, therefore, be eliminated or modified to govern the attorney's record only.

Here again, we have another peculiar problem. Does the reference point for a periodic downgrading begin after the application has been prepared from the disclosure or does the time start with the preparation of the disclosure from which the application was prepared? This can vary up to four or five years.

A third area to which management attention might be addressed is in the field of Patent Secrecy Act Administration. Here, there is a need for limiting the reviewing responsibility in patent applications filed by Defense Agencies or their contractors. Under the existing procedure, any member of the Defense Agencies can request the Commissioner of Patents to place any case under secrecy. The result may be that Navy invokes the Patent Secrecy Act in Army Controlled applications or Army invokes the Act in Air Force controlled cases or the Air Force threatens with, "You put one of mine under secrecy and I'll put two of yours under."

Control should be set up in a manner similar to the Defense Security Procedures in which the department having responsibility for the application, or the project, is the one that alone controls the use of the Secrecy Act. We have cases now that are just going back and forth between the different Services.

Finally, there should be a correlation made between the two security systems. There is no correlation at this time. As a typical example, we have a case that has been declassified under Defense Security procedures. Navy has just placed it under a Patent Secrecy Order. Thus, Army is carrying the subject matter as unclassified while Navy is controlling a patent application with the same subject matter under a Secrecy Order. There should be a consistent security posture with respect to such information. I propose that a set of regulations peculiar to patent applications be adopted by the Defense family, a set of regulations that is adequate and workable within the Defense Security and Patent Secrecy framework.

I also propose a committee, a coordinating committee, be established to

include members of industry that traffic in patent security matters, patent attorneys of the Defense family, members of the Patent Office Security Group, and security managers of the Defense family. Such a committee would provide a forum where problems that hinder the smooth working of the dual security systems could be resolved and the results incorporated into the respective regulations.

Remarks by Oscar B. Waddell —

My subject for the day is the "Impact of Security Classification and Patent Secrecy Orders on Processing Patent Applications from the Point of View of Industry."

These applications may fall within two categories: (1) those applications in which the government has a property interest and are classified by a defense agency under a contract; and (2) those applications in which the government does not have a property interest, but may be placed under a secrecy order by the Patent Office under the provisions of 35 USC 181.

Considering first those applications that are classified in accordance with the provisions of a classified government contract or Category I, let us look first, for example, at the provisions of Armed Services Procurement Regulations relating to classified government contracts.

According to title 9, paragraph 106, unauthorized disclosure of classified subject matter, whether in patent applications or resulting from the issuance of a patent, may be in violation of Espionage laws, 18 USC 793 et seq.

Accordingly, a clause must be inserted in every classified contract which covers, or is likely to cover, classified subject matter. This clause provides that before the filing, or causing to be filed, a patent application in the United States Patent Office disclosing subject matter which is classified secret or higher, the contractor shall forward a copy of the application to the Contracting Officer for determination of whether it contains classified subject matter. If nothing is heard from the Contracting Officer within thirty (30) days, the application may be filed.

For those applications classified confidential, special permission to file in the Patent Office is not required. However, the contractor shall furnish to the Contracting Officer, at the time the application is filed or prior thereto, a copy of the application for determination whether it should be placed under a secrecy order.

After the application is filed, the contractor shall furnish to the Defense agency the serial number and filing date of the application. When filing a classified application in the Patent Office, the contractor usually writes a separate letter identifying the agency and the number of the contract or contracts which require classification markings to be placed on the application.

It should be noted that the Contracting Officer shall ascertain the proper classification of the patent application. The Contracting Officer upon receiving the application's serial number and filing date shall promptly take the necessary steps to have the application placed under a secrecy order if it contains classified subject matter.

The classified government contracts referred to before usually have attached thereto a Security Requirements Check List which has been approved by the Contracting Officer. These check lists are of great assistance in determining the proper classification of the subject matter of a patent application. They are referred to in the Industrial Security Manual as DD Form 254.

The responsibility for the preparation of contract DD Form 254 rests with the Contracting Officer, not the contractor, but the assistance of the contractor is encouraged to help determine the appropriate classification. For example, the highest level of clearance for the contract may be secret; however, certain items appearing on the check list may be either unclassified or classified at a lower level such as confidential.

In addition, a detailed security classification guide may be issued. For example, in the manufacture of a jet engine under a classified government contract, various classification guides may be provided for each part of the engine and its performance. These guides are very helpful to the contractor.

In order to insure the time-phased downgrading and declassification, the classified material in the contract is assigned to a certain group by the Contracting Officer, such as Group 4, for example, which provides for downgrading at three-year intervals and declassification after twelve years. This information may be helpful later in determining whether or not a secrecy order should be rescinded.

Referring now to applications under which the government does not have a property interest, Category II, 35 USC 181 provides that if the national security is involved, the Commissioner of Patents may make the application available for inspection by any of the Defense agencies. If these agencies feel that publication or disclosure of the invention by the granting of a patent would be detrimental to the national security, they will notify the Commissioner and the Commissioner will order that the invention be kept secret and will withhold the granting of a patent for such time as the national security requires.

Thus, as has been pointed out, we have two different categories of applications that are placed under a secrecy order: those wherein the material for the patent application is originally classified under a classified government contract and those which are picked up by the Patent Office and placed in review for the Defense agencies to inspect. Further, in the first category, the application papers filed in the Patent Office have been stamped with the required classification markings and in the second category, the application placed under a secrecy order is not classified.

With further reference to the first category, the application is stamped on each page at the bottom and top with the required markings and each paragraph is not stamped as apparently required by paragraph 11 of the Industrial Security Manual. I do not feel that each paragraph should be marked. Patent applications are unique creatures in that they are considered as an entity. For example, a patent application may comprise: an abstract; an introductory statement which includes a reference as to what has been done before in the same field; a brief summary of the invention; a detailed description of the invention including the drawings, if any, together with specific examples; and the claims of the application which measure the inventor's protection.

If the invention referred to is classified, in all probability each and every paragraph would bear the same classification with the exception of the introductory statement which would probably be unclassified. As you can see, the parts of the application are interrelated and tied to the whole invention, and each paragraph depends upon each other to describe and claim the invention properly. To mark each paragraph would be a useless exercise and serve no security purpose.

Now, what effect does the secrecy order have on patent applications?

The problems associated with patent secrecy orders are many:

Unless the secrecy order is accompanied by a permit, the further development of the invention is made extremely difficult, if not prevented.

By its terms, the secrecy order prohibits foreign filing. While we can petition to modify a secrecy order to permit foreign filing, such petitions are not granted with respect to some countries like Japan and Spain. Even when the petition is granted, it is often difficult to file the application within the convention year, that is, within twelve months after filing of the U.S. application in this country.

The secrecy order prevents commercial sale of the invention.

The Patent Secrecy Order procedure and the contract security procedure are both attempting to accomplish the same end. Unfortunately, they do not always reach the same conclusion and there is an inherent time lag in the two procedures. Both can cause some peculiar results. For example:

A number of patent applications filed in connection with the TF39 engine were filed with Confidential markings and were placed under secrecy order by the Patent Office. Shortly before the scheduled C5A aircraft rollout at Lockheed, most areas of the TF39 engine were declassified by the Air Force. Since the Patent Office secrecy orders were still in effect, were it not for hurried up petitions to modify a number of Patent Secrecy Orders, the rollout would have then occurred with canvas shrouds over the engines.

Another example: A fuel injection device was invented in connection with an engine being developed under a government contract. The invention resulted in virtually smokeless engine exhaust. Under the government contract the device was not classified. However, the application was placed under a secrecy order. After several attempts we did manage to have the secrecy order removed and we were fortunate enough to have it removed in time to file within the international convention.

Another example: A patent application covering a low noise engine was placed under secrecy order. The concept was a commercial development and was not covered by government contract. No permit accompanied the secrecy order. Because of the restrictions on further disclosure of the concept, the secrecy order essentially prohibited further development. We managed to have the secrecy order rescinded.

Another example involves the synthetic diamond cases. The General Electric Company was a pioneer in making synthetic diamonds. For some unobvious reason, all of the diamond cases on file at that time were placed under a secrecy order. We filed petitions for modification of the secrecy orders for permission to file in countries with whom the United States had treaties to permit filing of classified material. Although many of the secrecy orders were modified, we lost several of our modified and sending the applications abroad to our agents through official channels. In some cases, such as in Japan and Spain, we lost our patent rights because we aren't allowed to file in these countries even though they have treaties; these treaties have not been implemented to allow us to file in these countries.

I feel that industry can live with the present security processes, because national security comes first. However, as in most cases, there can be improvements.

For example, it is felt that the countries in which classified material may be filed should be expanded to protect U.S. inventions, and, further, every effort should be made to have the countries such as Japan and Spain establish an acceptable procedure for protecting classified material.

If a patent application is to be placed under a secrecy order, it should be done promptly in order to give the applicant adequate time to have the secrecy order modified to permit foreign filing within the twelve-month convention date.

A simplified procedure should be established for the sending of our classified material to our cleared agents in foreign countries.

The petitions for rescinding and modifying secrecy orders should be considered as urgent matters at all times in order to protect the valuable property rights of the inventors.

The government should periodically review classified matter to determine if it could not be declassified or downgraded as required by amendments to Executive Order 10501.

Lastly, according to page 12 of the Industrial Security Manual, the contractor is required to show on what authority he is retaining classified patentable subject matter after the termination of a contract. A simple system should be established to review and dispose of such subject matter because patentable subject matter in the form of patent applications may be pending for years before the Patent Office, long after the termination of a contract.

Remarks of Roger L. Campbell —

I might mention that the name of the Security Group is now the Special Laws Administration Group.

Mr. Kelly and Mr. Waddell have covered all the points that I was going to raise so well that I won't bore you with repetition.

But there is one point that I would like to emphasize. That is that the Patent Office does not classify inventions or patent applications. We are merely the custodians or the stakeholders. We merely follow the Executive Orders and the statutes in protecting the inventions and the applications during the time that they are pending with us.

Questions and Answers —

Mr. Chelius (McDonnell Douglas): Mr. Waddell, under your first case situation, can the government — once a patent has been issued — then release to other contractors that patentable information, or the information that has been patented?

Mr. Waddell: The public, including the government, has access to all patented information but that does not give it the right to infringe the claims of a patent by using the invention.

Mr. Chelius: My second question is a case situation. The government presents a briefing setting forth a particular design problem without issuing a contract. Company A then undertakes on its own funds a development which is patentable. The government never purchases with Company A and perhaps award it to Company B. Does Company A have any rights against the government or Company B?

Mr. Waddell: Was the application filed?

Mr. Chelius: Yes, assuming the patent application was filed and put under an order of secrecy.

Mr. Waddell: After the patent has issued you can file suit to recover damages in the Court of Claims.

Mr. Chelius: What if the application is put under an order of secrecy?

Mr. Waddell: Well, there is nothing you can do as far as I can see except within the government agency concerned and the application is in condition for allowance.

Mr. Kelly: If it was put in what is known as a notice of allowability, it would not issue as a patent — and I

presume the thrust of your question was that it is wholly owned by your organization. You are entitled to any damages you can show beginning at that time that a case would be allowed as indicated by the issuance of a Notice of Allowability.

The Patent Secrecy Act has a provision under which redress is available to the owners of privately developed information that is withheld from being exploited because of a Secrecy Order; if damage can be shown, there is no arbitrary award — damage is the sole measure of compensation.

Mr. Chelius: Has there been an instance where a company has been able to establish damages?

Mr. Kelly: I'm of the opinion that such instances have occurred.

Mr. Florence: I'd like to ask Mr. Waddell two questions. The 35 USC 181, I believe it is, invokes the government invention and the private invention. And I, of course, understand how the government's application for a patent, the government's invention, would bear the government classification of Confidential or higher. What is there in law, or what is the basis in law, for there being an assignment of Confidential to a private invention?

Mr. Waddell: Well, I think at least the application would be not under a government contract.

Mr. Florence: Is there authority in law for someone in the government to impose some confidential marking?

Mr. Waddell: Well, they can recommend a secrecy order.

Mr. Florence: There is a distinction of course between a secrecy order being issued under the Patent Application Secrecy Act as opposed to the administrative marking of Confidential?

Mr. Waddell: That's right.

Mr. Neal (TRW): I don't know whether Mr. Kelly or Mr. Waddell brought this up, but is my understanding correct that you said there would not be both a secrecy order and a security classification on a patent application?

Mr. Kelly: I said something along that line that might have confused you. Remember I was talking about cases filed by the Army Material Command and controlled by it. This control permits flexibility in the timely application of a Secrecy Order. In cases filed by industry the government has no direct control over them and action is taken as soon as the application is filed.

Mr. Neal: Well, would there be this case with industry? Would there be both a security classification and a secrecy order?

Mr. Kelly: Oh, yes. Yes, it happens. It's the general rule on the cases. It happens as a general rule on these cases.

Mr. Florence: I'd like to follow through on this question which is sort of related to mine. I understood from Mr. Waddell that there is no authority in law for the administrative designation of Confidential even though the application for patent may qualify for a secrecy order.

Mr. Kelly: Now, let me get this statement correct. Where it is wholly privately owned — and you and I may disagree as to whether an application is or is not wholly privately owned — but where we both agree that it is wholly privately owned, there is no authority.

Mr. Loughran (Singer): Are there any circumstances where the Patent Office unilaterally would issue a secrecy order in the case of an unclassified government contract?

Mr. Campbell: No, sir. The provisions of 35 USC 181 require the Commissioner of Patents, where he considers that the grant of a patent for a particular invention might be detrimental to the national security, to

make that application available to an authorized representative of a defense agency. That would be the Atomic Energy Commission, the Department of Defense, or any other agency that is designated by the President as a defense agency. A secrecy order would be issued by the Patent Office only upon the recommendation of such defense agency.

Mr. Loughran: Following that up then, Mr. Kelly, would this impose upon the Department of Defense agency a requirement to classify the contract at this point, or to classify a portion?

Mr. Kelly: If it is privately owned, defense classifications do not effect it at all.

Mr. Loughran: No, this was exclusively an unclassified government contract at the point now that the secrecy order is recommended by the defense member of the committee — would it not be required that the user agency classify that?

Mr. Kelly: The answer to that question is yes, there should be a requirement on the basis of the spirit of security management. But there is nothing to tie together these secrecy provisions. That is one of the inconsistencies that I mentioned. There should be a certain correlation to the effect that you can't invoke one form of security without the other. We now can apply one form without the other and such circumstances shows an inconsistency in management.

Mr. MacClain: This question has come up before and it's simply a question as to whether or not an order of secrecy in and of itself, without anything else, would permit the imposition of a security classification marking, and the answer to that is no. The security classification must stand on something outside of and beyond an order of secrecy alone.

Question: But is the premise in both cases the same, that it is in the national interest?

Mr. MacClain: Well, yes, of course that's true. But the order of secrecy is statutory and the security classification is Executive Order, and the idea of having official information to which you could attach security classification may not exist at all in the case of information under a secrecy order.

To have security classification, it is essential that the government have an interest in the information either by ownership or control. It has been unofficially determined that the placing of a secrecy order by itself does not establish that degree of government control to justify security classification. There has to be something more.

Mr. Loughran: Well, I can see that in the case of strictly proprietary information but this is a case where we have a government contract involved.

Mr. MacClain: You are talking now about a case where the government is the proprietor of the information. But an unclassified contract, I would be a little bit at a loss to know why there was imposed a government secrecy order on it. I'd hate to say that that could happen.

Mr. Kelly: One reason why it can occur is that the individual who reviews the application for Patent Secrecy purpose is often a stranger to the contract and even to the department that spawned the contract. The procedural administration of the Patent Secrecy Act is carried out by submitting to the representatives of the various Defense Agencies those applications that come within the scope of categories in which they have expressed an interest. Thus, under this arrangement one department may review the application of a contractor of another department. Even within the same department, the filing of an application generated under an unclassified contract has a high probability of review by one unfamiliar with the contract. In view of this procedure, it is quite easy to

arrive at inconsistent positions within the Defense Agencies.

Mr. Loughran: Yet their representative on the committee recommended a secrecy order.

Mr. Kelly: On that committee there is an Army and a Navy man, and, therefore, they can all be interested in the same category, missiles. The Navy man looks at a missile area and says it's not. The Army man looks at it and says yes.

Mr. Richardson (Texas Instruments): One of our major objectives of the last few years has been declassifying as much as we can in the patent business. We have had a lot of residual information that has been just lying there. I know that the Patent Board reviews this stuff every few years to see if in fact it should be declassified. However, I can't say I have yet to have one declassified.

To whom do I go for quick and most effective declassification of information that caused a patent to be placed under secrecy order based upon a D254 statement? In other words, I've got a D254 or I've got a letter to declassify a whole gamut of programs. Now, the patent sits there with Confidential marking on it, still in secrecy. Who can I go to to get this thing declassified quickly?

Mr. Campbell: Well, I can't speak to you about how to declassify it because as I said, the Patent Office does not control or recommend or remove classifications. To remove secrecy orders, the procedure is simply to file a petition with the Commissioner of Patents to rescind the secrecy order and state whatever reasons you have for feeling that the order is no longer applicable. This then is referred to the defense agency which originally recommended the secrecy for reconsideration by them at this time.

Mr. Richardson: Then I should come to you. I should not go to the defense member and seek declassification or to get a rescission on the secrecy order. I should come to you and recommend rescission.

Mr. Campbell: Well, I'm not saying that that is the exclusive way to go. I don't know whether any other way would be quicker or not, but I don't mean to say that we are the exclusive agents here, that you must come to us. You may go directly to the defense agency if you know who they are.

The Patent Office, as I say, is merely engaged in the administrative handling of these cases. We do not have people who determine from the point of view of the Patent Office whether a secrecy order should or should not be issued. Cases come to our attention in the course of ordinary filing which the Commissioner feels ought to be reviewed for security purposes by a defense agency and we refer it to an expert of that defense agency. And we act solely on his recommendation. These people who make the decision as to whether the secrecy order should or should not be issued are not Patent Office people. They are defense agency representatives.

Mr. Richardson: You come to us and advise that the secrecy order is rescinded. But I have a Confidential patent. As far as I'm concerned, I can declassify that patent application based on that secrecy order.

Mr. Campbell: We cannot say that this is so.

Mr. Richardson: Well, what does prevent the patent from filing?

Mr. Campbell: We will not give you a patent which bears classification markings. I presume this situation: an application which bears security markings, has also been under a secrecy order under 35 USC 181. Now upon recommendation of a defense agency, the secrecy order has been rescinded. The markings remain on the papers. Our procedure in the office at this point is to write to the applicant and ask him either to

direct the removal of the markings or else inform us by what authority they are retained so that we can go back to the defense agency and get a new determination as to whether a secrecy order should again be issued.

Mr. Richardson: The reason I ask this is that it seems to be a lot of administrative hogwash to come to us and say, "You tell us why it should be classified; we're taking the secrecy order off." As far as I'm concerned, that's been reviewed by an appropriate official who has determined that that patent application is no longer classified.

Mr. Campbell: Our problem with that is that we have no way of knowing the authority for those markings. The secrecy order may or may not have been by the same authority. The authority which recommended the secrecy order and now recommends its removal may or may not as far as we know be the agency which authorizes and requires those markings. This is why we have to go to the applicant in every case.

* * * * *

CLASSIFICATION OF STARLIGHT SCOPE FROM INCEPTION TO HANDS OF USER

BY

MYRON W. KLEIN

The Army Small Starlight Scope, Figure 1, is presently being used in night operations by our troops in Southeast Asia. This resume is intended to give you some of the background for the classification rationale, to describe some of the significant components of this unique image intensifier device, and show their importance to the overall classification.

The Starlight Scope is actually a spin-off from the near infrared devices, or sniperscopes, first used in World War II, and which are still in active use by many European and Iron Curtain countries. The near infrared viewing systems utilized an infrared image converter tube, such as is shown in Figure 2. The tube utilizes an infrared sensitive photoemissive surface coated on the inside of the faceplate on which the invisible infrared picture is focussed. Electrons emitted from this surface within the tube are then accelerated and electrostatically focussed on a phosphor screen similar to that of a television picture tube, and the visible image which is produced is viewed by the observer through an eyepiece. As pictured in Figure 3, an infrared telescope incorporating such a tube requires an infrared spotlight to irradiate the scene with invisible illumination. All near infrared devices such as the weapon sights, Figure 4, have several serious drawbacks. They require a heavy battery or generator to provide the power for the spotlight, and they are only able to see the narrow field which is illuminated by the narrow infrared spotlight beam. The range, of course, is limited by the amount of power available for the light source, and an enemy similarly equipped can see the infrared beam with his own Sniperscope. These near infrared devices were classified Secret during World War II, were later downgraded to Confidential, and are now unclassified.

During the development of the tubes, it became obvious that their manufacture was an art rather than a science. Processes such as the chemical cleaning of the glass faceplate prior to depositing the light sensitive metallic coatings; the exact procedure for evaporating the coating; the temperature and time at which the tube must be baked for proper activation; were all very critical and extremely difficult to determine. To this day, the reasons for some of the steps in the process are not thoroughly understood. It was not until about 1952, after the expenditure of a total of several million dollars by the Army and Navy, that high quality infrared image converter tubes were able to be produced in such quantities that their cost was brought down

Figure 1. The Army's Starfield Scope

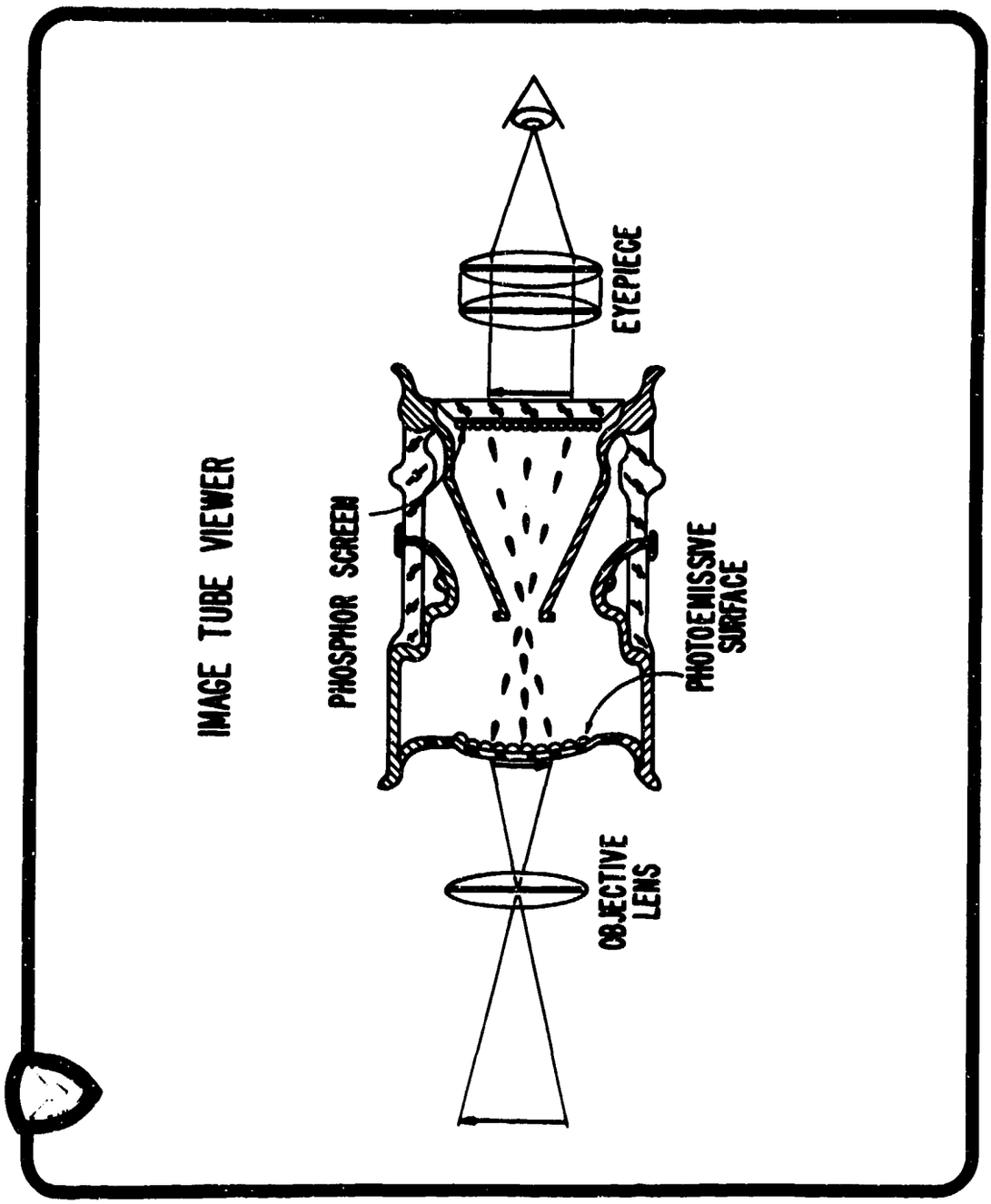


Figure 2. Infrared Image Tube Viewer

Figure [illegible].

Figure 4. Army Infrared Weapons Sight

to a reasonable value. Until very recently, none of the European countries were able to produce infrared image tubes of such quality and at a price as low as the United States. One can see that the key to placing in the field a fighting force equipped with such devices is really dependent upon the ability to manufacture these tubes. Consequently, the specialized manufacturing techniques were classified Confidential and have remained so until very recently, when it became obvious that the other countries had achieved the same capability, and that U.S. industry could gain financially from being able to lease some of its know-how to foreign affiliates.

The principle of the image intensifier tube, Figure 5, is essentially the same as the infrared image converter tube, except that the infrared sensitive photoemissive surface is replaced by a visible sensitive surface. A telescope using such a tube needs only the light from the moon, stars or sky-glow to make a clear, bright picture such as shown in Figure 6.

The Germans were known to have experimented with crude image intensifiers toward the close of World War II, and, although RCA in 1950 under Navy sponsorship, made the first attempt in the U.S. to build such intensifier systems, the technology in U.S. industry was not sufficiently advanced until about 1955, when the Army initiated a program to perfect these tubes. The early experimental tubes were unclassified. Their performance was not considered significant enough to warrant classification until about 1958 when the amplification or gain of these tubes was high enough and the resolving power great enough to be of military interest. At one point in this period, when it became apparent that industry would achieve extremely high gain, all tubes having a gain of over a hundred thousand times were classified Confidential. Very shortly after this, our laboratory experiments showed us that it was not gain alone which would make a superior tube, but a combination of gain, resolving power, and low background noise. For this reason, the hundred thousand gain criterion was abandoned in favor of classifying the individual performance characteristics.

During this same period, the astronomers who had abandoned the idea of building a telescope larger than the two hundred inch instrument at Mount Palomar were looking at the intensifier tube as a means of extending the capability of the telescopes already in use. The nuclear physicists who were looking for a means of amplifying the brightness of the faint flashes of light created by nuclear particle passing through scintillation chambers also had turned to the image intensifier tubes. Army scientists at the Night Vision Laboratory worked very closely with the astronomers and the nuclear physicists, and although the specific Army tube developments had to remain classified, there was enough general information which could be shared so that a cooperative effort proved to be worthwhile. Fortunately for the nuclear scientists, whose projects were sponsored by the Atomic Energy Commission, they were able to obtain security clearance which enabled them to share much more information with the Army than the astronomers who had to be satisfied with the unclassified spin-off from the Army programs. As it turned out, the Army abandoned a particular tube approach which was ideal for astronomy applications, and the astronomers, using funds from the Carnegie Institution, completed the development of their magnetically focussed cascade intensifier tube which is now available off the shelf and is being used on 20 or 30 medium-sized telescopes in this country and abroad. One of the astronomers recently stated that using these intensifier tubes, the rate of acquiring astronomical data by all telescopes in the entire world has been increased by over 100 times. The nuclear physicists on the other hand found new methods of recording the tracks of the high energy nuclear particles and abandoned their image intensifier program without ever developing an intensifier tube of their own.


IMAGE INTENSIFICATION
U.S. ARMY ELECTRONICS COMMAND
IMAGE INTENSIFIER
Reproduced from best available copy.

Figure 5.

[illegible] Starlight Scope

In 1960, a presidential committee cited the Army's lack of night vision capability as a serious drawback in its operations in Southeast Asia. A highly expedited development program was initiated to provide the Army image intensifier equipment in the shortest time possible. The key to such a program was the perfection and production of the modular cascade image intensifier tube, Figure 7, which up to this time had been proceeding rather slowly. Since one tube alone is not sufficient to give a bright image under starlight illumination, three tubes are placed in tandem so that each tube serves as a preamplifier for the next. Each tube amplifies the image brightness from 30 to 50 times so that the final image, which is emitted by the third phosphor viewing screen, is from 50 to 100,000 times brighter than the original faint image which was focussed on the photoemissive surface of the first tube. Although the original approach was to produce the three stage tube in one continuous glass envelop, overwhelming technical difficulties forced the abandonment of this method in favor of coupling together, through fiber optic faceplates, three individual tube modules. One or two U.S. firms had been experimenting with fiber optic plates, Figure 8, and they appeared to be a good candidate for the image intensifier tube coupling. For those not familiar with fiber optics, they are bundles of glass fibers in the form of either glass plates or flexible cables which enable one to pipe an image from one end of the fiber optic element to the other, Figure 9. Each individual fiber consists of a core of clear high-transmitting glass surrounded by a cylinder of a glass having a lower index of refraction. And, in many cases, a second cylinder of a dark absorbing glass is also used. A light beam which enters the core rod is reflected from the boundary of the lower index glass which surrounds it. The redirected beam continues down the rod and is internally reflected each time it strikes the boundary of the two types of glass until it finally emerges from the other end. Two inch diameter flexible fiber optic cables used for transmitting an image from one point to another have been made up to 12 feet long. In the case of the faceplates used for the image intensifier tubes, these fiber optics are fused into a solid bundle and then sliced into plates which are used as the end windows of the intensifier tube. A one inch plate contains about two million individual fibers. When the two or more of these tubemodules are butted together, Figure 10, the image from the first is piped directly into the faceplate of the second and similarly from the second tube directly into the third. Using these plates, all three modules could be made identical, which would not only simplify their production, but greatly reduce their cost.

The development of the fiber optic plates, which were required to be vacuum tight in spite of the fact that each plate was made of about two million individual glass fibers, all fused together turned out to be a formidable problem. An enormous amount of effort was poured into fiber optic R&D before plates of quality and vacuum tightness high enough for image intensifier tube production were produced. Here again, it was recognized that the process for manufacturing the fiber optic faceplates was the key to the producibility of the cascade image intensifier tube, and along with the plates themselves, their specialized manufacturing techniques were classified Confidential. At the time, there were few commercial applications for the fiber optic plates and the Army was the primary customer.

One problem did arise when the major supplier of fiber optic plates, who had been involved since the beginning of their development, objected to the Army's blanket classification of his product, especially at a time when he was trying to develop a commercial market. The classification of the plates was originally based on two criteria; one was the transmission characteristics of the glass; the

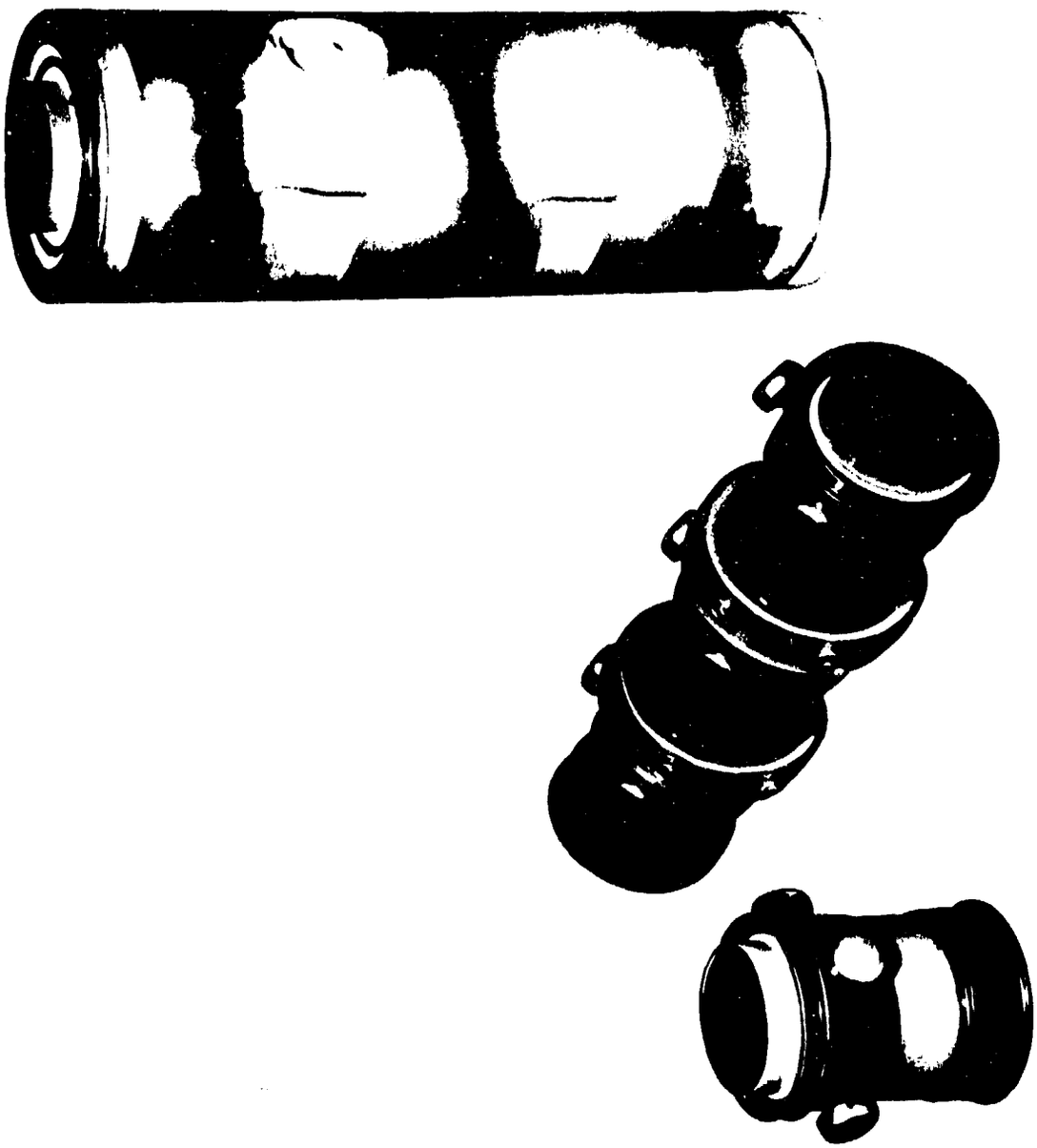


Figure 7. Cascade Image Intensifier Tube Showing Method of Coupling Tube Modules

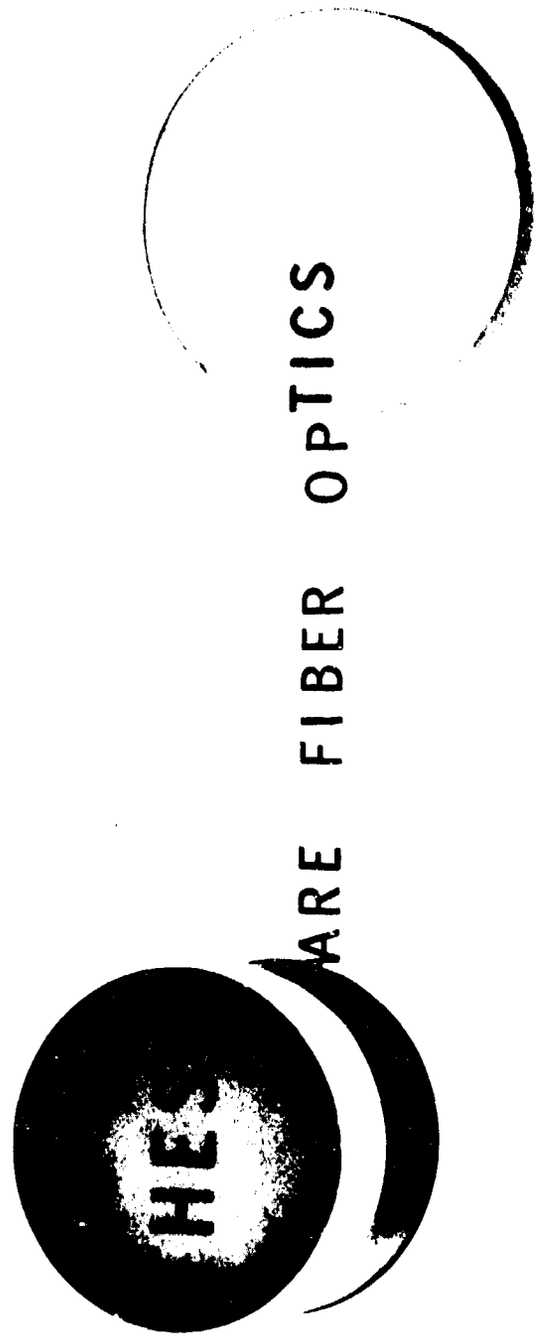


Figure 8.

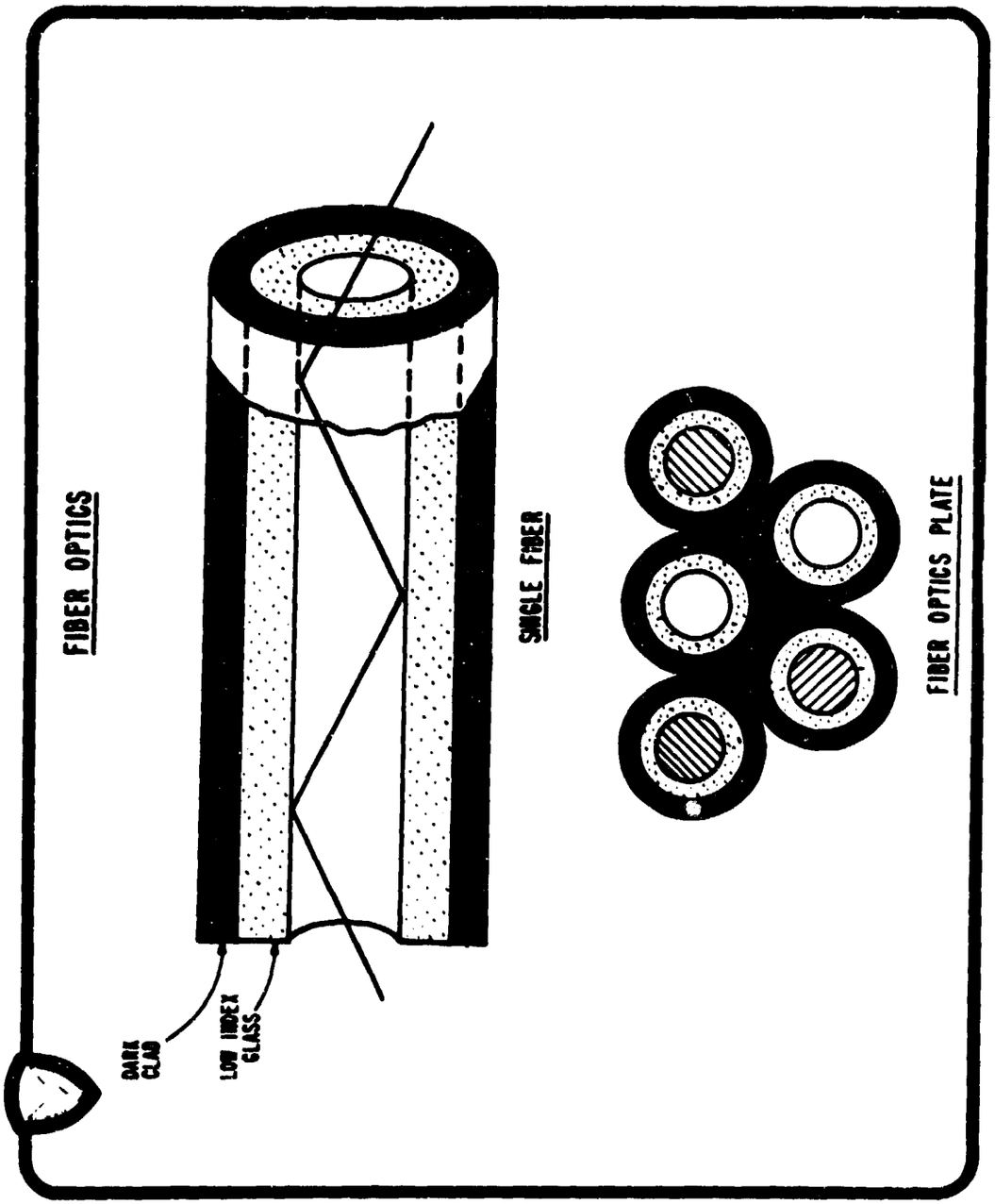

FIBER OPTICS
SINGLE FIBER
FIBER OPTICS PLATE
DARK CLAD
LOW INDEX GLASS

Figure 9.

Intensifier Tube
fiber optics
photocathode
fiber optics
phosphor screen
lens
target
IMAGE INPUT
fiber optics
photocathode
phosphor screen
fiber optics
phosphor screen
lens
eye
INTENSIFIED IMAGE OUTPUT

Figure 10.

other was the chemical compatibility with the light sensing surface which had to be applied to the plate after it was incorporated into the tube. After about five months of correspondence and discussions in which the DoD Directorate of Classification Management served as the mediator, the problem was solved by differentiating between the high resolution plates needed by the Army and a lesser quality which could be used for commercial applications. The new classification criteria consisted of four specific requirements which the fiber optic plates had to meet in order to be considered classified. These consisted of the original transmission and chemical compatibility as well as another optical property called edge response, and a minimum fiber diameter. Any fiber plate which satisfied all four requirements was considered Confidential.

In November 1964, news releases resulting from a press conference which was held at the Pentagon showed that the Army might be revealing information which could provide a fairly good estimate of the Army's technical status and readiness in the night vision field. The policy which finally evolved was that until the U.S. learned the status of such development in Iron Curtain countries, publicity on night vision equipment was undesirable, and further types of information to be withheld included military applications such as use by Special Forces, employment on various weapons and other military tactical situations. Also to be excluded were performance and technical characteristics including range, design details, size of optics, magnification, resolution, brightness and amplification, from which military performance could be derived. The power supply, which although somewhat unique in its ability to produce the 45,000 volts from a small dry cell did not represent any technology not available throughout the world. It therefore remained unclassified along with the batteries, lenses, and other conventional components which made up the rest of the telescope.

As the development progressed and military users were receiving Starlight Scopes for test and evaluation, it became obvious that some sort of a security classification guide was needed. Up to this time, security check lists, the DD Form 254, had been supplied to the contractors, but no security classification guidance had been distributed to the military users. As an example, the initial production of 2000 Starlight Scopes was to be provided to the Army Combat Development Command Experimentation Center for large-scale tests. Large numbers of troops would require security clearance, and facilities for storage and issue had to be arranged. A security classification guide was prepared with the user in mind, covering the night vision systems and their components. It clarified the classification of the unique and unfamiliar parts as well as often confusing items such as imagery taken through the systems. Although the guide may have been restrictive to some, it clarified the handling of the equipment and was welcomed by security officers at many Army installations.

Toward the end of 1965, the Starlight Scopes which were being built for the troop tests were diverted to Southeast Asia, and commanders were suddenly faced with the problem of storing and issuing classified devices on the actual battlefield. This also proved to be a considerable burden for the Sacramento Army Depot which was responsible for the issue and maintenance of the devices. An electro-optical device facility which had been set up in the depot for maintaining unclassified conventional optical devices had to be revamped so the classified Starlight Scopes could be handled. This, of course, required more personnel in addition to the bars on windows, locks, and security storage containers.

Handling the scopes in Vietnam proved to be even a more difficult problem. Shipments of scopes to and from the depot were accompanied by courier and signatures were required every time the shipment changed hands. At training centers a clearance was required

for troops so that they could be issued the Starlight Scopes. In actual combat zones troops going out on night patrol had to sign for the scopes just prior to leaving their company area and often were given no time for familiarization or even boresighting their weapons. There are reports that some commanders who received shipments of the scopes never even opened the cases, since they felt that the encumbrance of all the security precautions would hinder the accomplishment of their mission.

In spite of all these problems, exciting stories filtered back from Southeast Asia. In one case, a U.S. soldier observing one night through his Starlight Scope saw a Viet Cong preparing to implant a mine along a dirt road. The GI watched until he saw the Vietnamese pick up the mine, at which time he fired his rifle and actually detonated the mine in the man's hands. In another case, a night reconnaissance patrol equipped with a Starlight Scope detected a company of Viet Cong moving up the road toward them. As the patrol prepared an ambush, the observer with the Starlight Scope discovered a second company a short distance behind the first. The patrol leader allowed the first group to pass and then ambushed the second group. The first group, hearing the shots, returned to the ambush site and entered the fight. In the confusion, the two groups of Viet Cong fired on one another while the U.S. patrol withdrew and called for artillery fire on the Viet Cong. The platoon sergeant credited the Starlight Scope with saving the lives of the patrol. It was stories such as these which convinced the Army authorities that the image intensifiers, when issued in a great enough density, would make a significant improvement in the Army's night fighting capability. On the other hand, it was easy to see that the security classification was certainly restricting their general use.

In the spring of 1967, in order to give more latitude to field commanders in utilization of the image intensifier devices, the Army reclassified the first generation image intensifier devices Confidential, Modified Handling Authorized. Although this classification seemed questionable to many, it gave the commanders in the field the flexibility which was needed in order to carry out their mission effectively. Finally in 1968, a message was received from Southeast Asia which indicated that since a sufficient number of the new devices had been lost and presumably compromised, it was no longer of any value to maintain the Confidential classification. The Army agreed to declassify the equipment, but, noting the rise in crime throughout the U.S., petitioned the Office of the Attorney General to limit the sale of the new devices so that they would not fall into the hands of criminals. Although the Attorney General's Office was sympathetic to the Army's concern, it pointed out that since the Government is presently unable to control sales of items such as firearms, telescopes, binoculars, infrared apparatus, bullet-proof vests, and clandestine listening apparatus, it would be impossible to control the image intensifier devices. As a result, the Army directed that throughout their life cycle the image intensifier devices will be controlled items of equipment and that in future procurement of the systems and image intensifier tubes, instructions should be provided to control overruns and for disposition of equipment not meeting specifications. Procedures were established within the Army to control the issue, use and disposition of equipment while in service as well as when rendered unserviceable. Although the Army still takes these precautions to control the image intensifiers in its possession, there are at least three U.S. firms which now market commercial versions of these telescopes, and the intensifier tubes themselves can be purchased commercially both here and in several countries in Europe. Only the high price of the devices maintains some measure of control over their civilian use.

In reviewing these highlights of the classification events in the development cycle of the Starlight Scope, it

is felt that the actions were reasonable and considerate of industry's position in the commercial market. As in any security classification program, one can never know how effective they may have been. There are no control experiments such as are used in physics, chemistry, or biology. There is always the question of what would have happened if the Army had never classified the Starlight Scope. They might have become available commercially perhaps one or two years earlier, but it is very doubtful if the present prices would have been reduced substantially.

* * * * *

WORKSHOP A — LIFETIME CYCLES FOR SECURITY CLASSIFICATION

Remarks by Jerome H. Kahan —

I would like to pose and discuss three propositions on the subject of classification, and then draw some general conclusions on security guidelines.

1. There is a legitimate need for classification — whether this is taken to mean classification of certain military data or protection of certain policy deliberations and decisions.

2. Despite the admittedly excessive amount of Executive Branch classification which exists, the public and the Congress have always been able, and will continue to be able, to gather sufficient information, both factual and conceptual, to understand many national security and defense issues well enough to question Government decisions and to offer counter suggestions.

3. Nonetheless, for a number of reasons, the Executive Branch is overclassified and should seek to revise and loosen the criteria for classification.

1. The Need for Classification —

I would like to explore this question by separating military-technical problems from policy issues. Although this distinction is often artificial, there are important differences which should be borne in mind.

The national security needs for keeping certain military information secret are obvious. Consider, for example, data which could endanger the survival of our nuclear forces — such as information on possible system vulnerabilities. If this information were made available, we could come to doubt the reliability of our own deterrent. Coupled with the fact that we are facing an adversary — the Soviet Union — who relies to a far greater extent than we do on secrecy, this could increase the chance of nuclear war by creating a serious imbalance. Even a small increase in the risk of a breakdown in deterrence cannot be ignored, whether it arises from a "real" situation or simply flows from the percentions of Soviet leaders who may erroneously conclude that they could negate a large fraction of our missile force and then be prone to take dangerous actions.

Many people interested in arms control advocate greater declassification. Yet, if we opened up all of our information regarding the manufacture of nuclear weapons, we would be in violation of the Non-proliferation Treaty and would make it easier for other nations to get nuclear weapons. In some instances, therefore, full freedom of information can run counter to the goals of nuclear stability and arms control.

On policy grounds, there is also a need for classification — although I hesitate to use the term "classification" in the respect. Perhaps the problem should be thought of as the need to keep private certain government deliberations and decisions on important policy, diplomacy, and negotiating questions.

The Government serve the public interest, but it cannot perform this func-

tion unless government officials have a certain amount of privacy in the process of decision making. This is not unusual. I am certain that the IBM executives would not like their marketing decisions to become totally or prematurely visible. And I am equally certain the New York Times would hesitate to publish in detail their internal deliberations regarding the decision to publish the "Pentagon Papers."

If U.S. officials cannot count on a certain amount of privacy within the Executive Branch, freedom of expression might be inhibited. This could lead to adverse policies, since decision makers might not be made aware of all the relevant facts or alternative courses of actions. Moreover, the lack of privacy might prevent the results and rationale of important policy decisions from being set forth in writing. This, in turn, could cripple the effectiveness of the bureaucracy in carrying out desired policies.

What if the "SALT Papers" were thought to have a high probability of being "leaked" en masse in a few years? What would happen within the U.S. Government in terms of SALT policy making — to the arguments that are being made, to the writing on the pros and cons of the various options that are being considered, to completeness of the final policy papers? Decision making might well be inhibited to the point that the prospect for reaching agreement could be harmed. And if something like this were to appear at a time when an agreement was put up for Senate ratification — perhaps by someone who thought that the agreement was "no good" and was trying to expose this fact — we could conceivably lose the opportunity to achieve what might in fact be a very fine SALT agreement.

A certain amount of privacy is also needed in dealing with other nations. There is nothing new about the fact that negotiations with other nations generally tend to be conducted in privacy, with the public on both sides not usually apprised of the details. Complete openness could endanger the ongoing international negotiations. For example, the Soviets have already complained about the "leaks" on SALT in the U.S. press. Furthermore, negotiators often use the tactic of preparing "fall-back positions" which you may plan on using in a later stage but which you do not divulge at an earlier time. As in the case of labor-management negotiations, this information cannot be subjected to public scrutiny while the parties are bargaining.

2. Availability of Information —

Despite the existing classification structure, a wealth of material is available to the public and the Congress on national security issues. At Brookings, I have analyzed the defense budget, strategic policies and concepts, various weapons systems options, and the SALT negotiations. I have not been using classified information; I have been relying upon newspapers, journals, and general knowledge. Information can also be found in Congressional testimonies, the writings and speeches of former Government officials, and through official "leaks" emanating from the Administration — both inadvertent and deliberate.

Important national security issues often do not require detailed military data, but a knowledge of concepts, a sense of history, and an awareness of current international problems. Indeed, it may be more essential for the public to understand the principles and fundamentals behind policy decisions than the specific facts. Often, the "facts" are not known with certainty within the government. For example, officials in the Executive Branch may not know all the facts about our weapons systems, and the intelligency community is constantly arguing over "facts" regarding Soviet capabilities and intentions. In any event, whether inside or outside, one does not need to know all the facts to make sound judgments.

As an example, consider the Sentinel ABM issue in 1967. Sentinel was Safeguard under a different name and with a slightly different configuration. When the Johnson Administration announced that decision, there was a minimum of public awareness and debate — especially when contrasted with the tremendous public outcry and Congressional fight over President Nixon's Safeguard ABM decision in 1969. I do not believe that lack of information can explain this difference. Open sources available in 1967, including Secretary McNamara's own statements, provided a great deal of information on ABM capabilities and rationale — the "anti-China" argument, the effect on arms control, the approximate system cost and effectiveness. The fact that the decision was about to be made was known to anyone reading Secretary McNamara's official statements or simply following newspaper reports. It seems clear that the lack of debate over Sentinel was due to a lack of public and Congressional interest.

In the case of President Nixon's Safeguard decision, on the other hand, the public was made aware of the issues, principally through the efforts of many foreign policy and technical experts who were critical of that decision. Significantly, those critics did not need specific information on the Soviet MIRV threat to argue their case, but raised many basic policy questions — for example, whether Secretary Laird was justified in expressing concern over the possible "loss" of our ICBMs when our Polaris and bomber forces would remain secure. This is not a classified issue; it is a conceptual issue. And Government officials, having access to all classified information, disagreed on the subject of whether we should deploy Safeguard in order to maintain a sufficient deterrent.

3. The Need for Greater Openness —

Notwithstanding the many genuine needs for restricting the availability of Executive Branch information, a far greater degree of openness is essential. At least four reasons support this judgment:

First, under the present system, Administration officials have an advantage. They do have more facts and more analysts than the public, and, equally important, they receive more publicity. A policy statement made by the Secretary of Defense about our doctrine of sufficiency, for example, carries more weight than statements of the loyal opposition. As indicated, it is a mistake to believe that because the Administration has more information it can make sounder decisions. We can take away some of the Executive Branch's misplaced "credibility advantage" by opening up information to the public.

Second, continued reliance on "leaks" and newspaper analyses of "hints" dropped by Dr. Kissinger is a very unreliable and chaotic way for the public to acquire national security information. It depends on a particular reporter, a particular official, or an individual reading a specific journal article. I work at it full time; but how can a Congressman or the interested man on the street confidently piece together the puzzles? Thus, there is a need to make more information systematically available to the public.

Third, the public has a right to know and comment upon fundamental Executive Branch decisions which affect the basic security of this nation. If there is an abuse of classification, whether for military reasons or for policy reasons — including misjudgments, deceptions, or half truths — it needs identification and correction. In crucial decisions concerning war and peace, the Government clearly has a responsibility to do more in exposing its decisions to public scrutiny and public approval.

Finally, the process of Executive Branch decision making can be improved through a selective reduction of secrecy. Those who work in the Government tend to develop a feeling which can best be described as "Executive

Branch arrogance." Only you — and the other bureaucrats working on a problem — know what is best. All the reasons for a particular policy must be valid, because they appear in a National Security Memorandum. Through this phenomenon, officials may forget that some of their assumptions were tenuous, that circumstances may have changed, or that they may be wrong. As a result, the Government makes too many unsound decisions and adopts too many policies which lack wide public support. Only inputs with a different perspective — Congressional, public, and outside experts — can solve this problem.

How can we go about a selective reduction in secrecy?

As a minimum, the Executive Branch should go out of its way to be more candid in its public statements, to consult with Congress in a more systematic way, and to get the advice of experts outside the Government. This is not a classification question, but an attitudinal question on the part of the Executive Branch. In any event, many Congressmen and Congressional staff members have security clearances and can be given access to secret information. Thus, independent of any corrections in the present classification system, a great deal can be done immediately to increase public education and involvement on national security issues.

At the same time, the Executive Branch should loosen the criteria for classification. One way of approaching this problem might be to develop separate standards and systems for military and policy information. Another might be to introduce "functional categories" and decide what level of classification, if any, is needed, keeping in mind the distinction between policy and military information within each category. Consider these examples:

— Foreign policy objectives and broad diplomatic options should be kept open to public discussion, but specific tactics associated with ongoing negotiations should remain sensitive.

— The methods used in analyzing our defense needs and the plans for our future posture should be made public, but detailed calculations dealing with specific aspects of cost and effectiveness might be kept limited.

— Basic R&D probably should not be classified, but specific future weapons' plans and developmental efforts on certain kinds of weapons might continue to be classified.

— Overall deployment plans and strategic doctrine do not need classification, but operational targeting plans and command arrangements need security.

— General estimates about the "Soviet threat" should be declassified, but detailed estimates on Soviet weapons' characteristics might remain secure.

— Highly-specific techniques of gathering intelligence should remain classified, but our overall ability to assess the military capabilities of our adversaries could be safely exposed.

These examples simply illustrate a possible approach. Whatever system is used, however, when facing decisions involving classification, I believe that we should ask two key questions:

First — how might the release of any information adversely effect the security of the United States in military-technical terms, or in policy-diplomatic terms, in the short term and in the long term?

Second — what is the positive value in making this information public, based upon the reasons discussed earlier — in essence, the public's right to know and the need to get "feedback" on decisions.

These two countervailing needs have to be balanced against each other — the legitimate need to classify versus the legitimate need to declassify. When this judgment is made on the side of classification, I believe that there is an obligation on the part of the Executive Branch to explain why and to ensure that items which should not remain classified beyond a certain period of time are made available publicly.

Remarks by Dr. Stephen J. Lukasik —

My purpose in being with you today is to discuss the relation of classification to research and development and, in particular, the time-dependent aspects of the problem.

It is generally believed that unrestricted communication maximizes the rate of research progress. Though unproved, and probably unprovable, let us accept it as correct. One then argues that classification systems, by impeding communication, are detrimental to progress. Before agreeing, we must ask two questions:

1. Communication between whom?

2. Is unrestricted communication a necessary or a sufficient condition?

The answer to the first question, communication between whom, is, "The relevant community." To the extent that this community is identifiable a priori and the security system is flexible enough to accommodate an adequate number of people, no problem in communication ensues. However, if the relevant community is not identifiable a priori or if the security system is not sufficiently flexible, then a loss in communication may result from the exclusion of an important or even vital part of the manpower/facility pool that could solve the problem. It may even prevent the solution of the problem.

How serious is this problem of identifying the relevant community? On the whole, I would think it is not serious for three reasons: first, a program so ill-planned that one cannot identify the resources required before one starts, which means that one is apparently relying on either divine intervention or just plain luck, strikes me as being poorly managed and one that has dim prospects for success anyway. Second, the security system admits within it a number of high-level advisors who serve to carry the word from one isolated group to another. Thus, major sins of omission or commission are unlikely to persist. In fact, such a system may be a better way to organize technical planning and communication rather than the great flailing about that results when everyone talks to everyone else. And third, it must be recognized that the security system consists of professionals embedded in a matrix of related unclassified work. Thus, the unclassified work that may be relevant is there to draw upon and it only requires the time to search the unclassified world and the wits to recognize its significance. When the research is revolutionary and highly classified, there is no external community to be concerned with but this is more the exception than the rule and, in this case, the relevant community is, by definition, identified. The latter point, concerning wits, is probably the more serious one, since closed communities, either social or intellectual, have a tendency to atrophy if they are below some critical size. And the more highly classified the subject, the more likely it is that a critical size community will not be assembled. That, however, is a detail of management and not a crucial fault in the concept of a classification system.

The second question, whether unrestricted communication is a necessary or sufficient condition, is perhaps the more interesting one, and one where we have various sorts of theoretical and experimental insights. However, despite our information on the subject, it is still very much of an open question. There are examples where a highly effective compartmentalized security system has turned

out excellent results, even in revolutionary areas, such as nuclear weapons in the early days. Also, we see a sufficiently effective Soviet system working under wraps and working well enough to cause us a great deal of worry. Thus, I am inclined to view the question in a purely empirical way and conclude that unrestricted communication is a sufficient condition rather than a necessary condition to achieve an adequate rate of progress.

The next question then is one of efficiency: Is a restricted communication system optimum in terms of speed, cost, effectiveness, etc.? These again are probably unanswerable in the sense that it is unlikely that valid controlled experiments will ever be undertaken nor does behavioral theory offer much of definitive understandings. But if you will accept another purely personal and intuitive comment, I think that the basic characteristic of human creativity dominates the research and development process and the optimization questions represent worrying about the second-order terms in the equation.

Turning to the question of time scales, there are two ways of looking at the relationship between security classification and the lifetime of classification information. I will try to be precise, but I must admit at the outset that these concepts do not lend themselves to either quantification or precision.

The first way of viewing the question is to define lead-time as the time interval between when an adversary would do something if he had a piece of information and when he actually does it after eventual receipt of the information. The delay in an adversary's action or counter is presumably what a security system buys you. In order to understand lead-time, it is necessary to look into several time intervals. These are:

Basic Research Time — May or may not be classified but probably is not.

Development Time — Likely to be a classified activity, mainly due to the end use rather than anything inherently classified about the activity.

Field Test Time — At this point a weapon system is often accessible to various intelligence-collecting devices.

Production Time (including decision-making time).

Deployment Time — That is, the time when one has enough deployed to be militarily significant.

Period of Utility — For ships and aircraft this alone can be 10-20 years.

The point is that classification can buy you some time; for large weapon systems the time is mainly equal to the development time plus as much of the field test time as it takes an adversary to figure out what you are doing; for a small system it may be somewhat longer but the whole issue may not be terribly important in such a case. This time is worth something but it may or may not be crucial. If the development time is long, and if the adversary is very far behind in that technology, and if the U.S. uses its lead to push on to more advanced systems, then the time is worth a great deal. On the other hand, if these conditions are not satisfied, the time may be worth very little in the long run.

The second way of viewing the lifetime question is concentrate not on what an adversary does but to simply follow the information itself as it travels from the generator to an adversary. This time has as a lower limit the normal communication time such as in the absence of a classification system. It is the amount of time it takes for news to spread under conditions of unrestricted communication. Assuming some modicum of effectiveness of a security system, the lifetime exceeds this lower limit by some amount determined by four possible

actions:

1. Independent discovery by an adversary

2. Inadvertent disclosure, i.e., the security slip

3. Unauthorized disclosure, i.e., spies and leaks

4. Authorized disclosure, i.e., declassification

Depending on circumstances, the additional lead-time provided by a classification system can be quite short, as is the very common situation when technologically comparable adversaries start off from the same base and proceed in parallel ways that are universally obvious to technical people.

Thus, an important point is to examine the position of our adversary. If we think our adversary is slightly ahead of us, it is probably better to take off all limitations on our people and give them the rein on the assumption, admittedly unproven, that unrestricted communication is worth something. But if we are far ahead of or far behind our adversary, then it is well to classify. In the first case, we protect a lead, and in the second case we conceal a possible vulnerability.

Finally, I would like to touch upon another aspect of the relationship between R&D and security, namely, the question of what I will call existence theorems. Often the only thing it is useful to conceal is the existence of a feasible possibility. Once this is established, it is usually easy for a technical man to duplicate the achievement. Aside from the fact that certain technical facts concerning the approach are then usually available also, there is the psychological effect of knowing that a solution exists and someone of presumably modest capability has already achieved it. On the other hand, one must admit that it is risky to make the best-case assumptions that we know something that our adversary does not.

In summary, I would make the following recommendations:

1. One must handle classification on a case-by-case basis.

   (a) Fixed short lifetimes have a weakness in those cases where a long lead-time exists on one side or the other.

   (b) But unlimited lifetime is unrealistic.

   (c) One should interact with the intelligence community and use adversary positions as a consideration in making classification decisions.

2. State why each document is classified as part of the document.

   (a) It requires the classifier of the document to be informed and to think through the problem.

   (b) It guides users of classifying derivative documents.

   (c) It materially assists in the declassification process.

Remarks by Frank J. Thomas —

As Steve Lukasik was talking, I was busily taking notes that I was going to use to shoot down his arguments. Then he ended up with conclusions that I agreed with wholeheartedly, so I decided to throw away the notes and try to add something to the arguments rather than shooting them down.

I want to start off where I ended with this group five years ago. As Steve mentioned, if I wrote it down a few years ago, it must be right, because it is still there on paper.

What I said in the summary of the talk I gave this group five years ago was:

1. An effective classification policy must include consideration

> of the effect that possible restrictions of information will have on other technical developments. Such restrictions will necessarily have some adverse effect on the development of your own systems for national defense and national security.
>
> 2. Such restrictions will also necessarily have an adverse effect on the growth of the economy as a whole and national security is not unrelated to this growth.
>
> 3. That the requirements for national defense in an absolute sense are not ends unto themselves but must be balanced against other necessarily competing requirements such as justice, liberty, and general welfare.

I still believe most of those points. We cannot operate in a vacuum, thinking only about national security or our position vis-a-vis the Russians. We must look at classification in a general and broader sense and think about how the whole economy moves, how the society advances, and what our society is all about.

A recent Supreme Court decision paid you gentlemen a very high compliment. The issue was a very difficult one involving classification.

Potter Stewart said:

> The Executive [Branch] must have the largely unshared duty to determine and preserve the degree of internal security necessary to exercise that power successfully. [He was talking about the power to classify and control information.] It is an awesome responsibility requiring judgment and wisdom of a high order. A very first principle of that wisdom would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless and to be manipulated by those intent on self-protection or self-promotion.

I agree. If we have a security system that does not appear to work, if people continually see leaks to the newspapers, leaks to the press, leaks to the Congress — then people do become cynical and careless, even though those leaks they see may not be important.

Let us go on to classification time, which is the subject of this discussion. The Office of Scientific Research and Development in 1946, at the end of World War II, published a report on their activities:

> In the midst of war, it is clear that the best security lies in speed, in achievement, rather than in secrecy. That this secrecy can defeat its own purpose is shown by the frequency with which enemy scientists independently discovered techniques zealously guarded by us. Our secrecy merely slowed down our own production and decreased our time advantage.

This was at a time when science had been moving very rapidly. In things like radar, bombs and guidance, technology was going very, very fast. The scientists who were engaged in research at that time concluded that it was best to run free and open and to try and stay ahead of the adversary just by having better scientists working on better problems.

A lot of that is still true today. We do inhibit our own development, in many cases, by only allowing a very limited group of scientists or individuals to look at a problem, by restricting some of our brightest people, who may be sitting on the campus. If these people are not exposed to these problems, they will not be coming up with the solutions. And it is solutions you want. You want solutions so that the whole process can move ahead faster.

There are specific areas that I will talk about later in which, I am sure, you do need classification.

In physics, science very often comes up with a measure of time we call the "characteristic time." It is some sort of fundamental time of the process. Now in classification, the process that we are talking about is dissemination of information. I tried to look at the characteristic time of information flow, and how it affects the declassification decisions that we might make.

I would suggest that one characteristic time for information transfer is the number of people in a field divided by the rate at which these people have to have this information in order to do the job adequately. This characteristic time could be very long if only a very select few people need to know that information. On the other hand, if the rate approaches infinity — that is, if a very large number of people need that information in order to do their job adequately — then the characteristic time associated with that information becomes very short. It is similar to the diffusion time that Steve was talking about. If the information is going to be, or should be, disseminated to a very wide group of people, then the best way is to disseminate that information is in the open. Put it in Physical Review or whatever journal seems appropriate.

Another characteristic time is the useful life of the gadget, the fundamental time that a piece of hardware has a use. That, of course, varies again. But in general in national security it is likely to be measured in years, not decades, particularly if you are in a fast-moving technology.

Another characteristic time is determined by the duration of a force vulnerability.

What we really want to do is to prevent an adversary from taking advantage of force vulnerability. So the time that we are talking about is related to how long it takes to fix that vulnerability, or how long a particular item is vulnerable. For example, if you find that a Minuteman won't come out of the whole, that is pretty important. You probably should try to fix it as soon as possible, and you probably should not publicize the fact until after you have fixed it. The same with military deployments. If you are exposing men to risk, if you are exposing them to fire, you must protect them while they are vulnerable. But after the mission is over, it probably matters very little whether or not the details of that particular mission come out. The vulnerability time constant has to do with the time of the vulnerable exposure.

Another fundamental time in our society, on policy issues in particular, is the time between which the citizens of the United States judge their representatives. The time is roughly the four-year time constant of our election process. It is not clear whether the classification time on policy issues ought to be shorter than that, so that all of the returns are in at each election, or should be longer than that, so that an Administration does not have to justify each and every decision. But the time constant is roughly four years, plus or minus a little.

In going over some of these characteristic times, it would appear that most of them are shorter, sometimes much shorter than our declassification times. But we very quickly get to what Steve mentioned, that decisions must be on a case-by-case basis really. An individual must go through and try to make a decision as to how long that particular secret is likely to stay secret, or how long it should stay secret.

My general thesis then is very much as it remained, as it was five years ago: that research and development activities proceed best if you are running free and out in the open, with free dissemination of information, so that everybody is informed of the problems and the possible solutions. Now going fastest isn't necessarily the same thing as being ahead of your adversary, but it is

often very close.

I have a specific proposal to make to this group. I don't know what the proper number is, but I would guess that something like 80 percent of all of the information that is now under some sort of security wraps could be, and should be, declassified. Either the information doesn't matter, or it is obsolete, or the adversary will get the information without a whole lot of trouble anyway, or he will independently discover it. This would eliminate for the technical man a great deal of the present work of maintaining the security of most of the data. For the remaining 20 percent of the information, I would require that each classified document have a very clear paragraph that states the justification for classification on an individual basis. It would describe why the information is classified, what the rationale is, so that a person making a derivative document has appropriate guidance.

What would those justifications be?

1. Intelligence Information

Intelligence sources obviously need to be protected. If you have a source of important information, and if your adversary can and would close off that source of information, then you must protect the source or lose the data. Classification times could be long.

2. Force Vulnerability

As long as you have a section of your military force that is vulnerable, and the vulnerability could be exploited by an adversary, the information should be protected. The time requirement is probably much shorter than for intelligence information.

3. Treaty Requirements

If you have agreed with country "X" to protect a certain bit of information — the fact that you have some sort of a joint force or an installation in a particular place — then you have to protect that as long as you have that treaty. Perhaps you should minimize the number of secret agreements, but so long as you have made such an agreement, you must abide by it. The justification paragraph should explain that we are protecting the fact that "Y" installation is in country "X."

Now let me say some of the things that I would not necessarily protect:

I would not necessarily protect force levels. A primary object of military forces very often is a deterrent. If the deterrent is going to be successful, you have to communicate the existence of that force. You have to make that force credible to the adversary. So let him know about it. Tell him.

I would not classify technology in which you are behind, because the best thing that you can do there is run as fast as you can and try to catch up. I would not classify technology in which you are even. I would not even classify technology in which you are a little bit ahead, because if you are a little bit ahead, the best way to stay a little bit ahead is to run faster than the other guy.

Classification may be desirable only in areas in which you are far ahead. If the technology has a critical importance to national security, and you would not like your adversary to have that advantage — then protect it. But as soon as the other guy discovers that principle, there may be very little point to classification any more. Or are you describing a particular piece of hardware? As soon as you begin to deploy it, the other guy may see it and realize what you are doing. At that point then the usefulness of classification comes to an end.

The classifier should recognize and record what he is protecting: Is it hardware? Is it an idea? Is it a decision? Is it a policy?

This may sound like a lot of work, having to think through each case and to write down the rationale. I think

that it should not be any more work than we are now doing, because at some point in every system, somebody has to think through the classification, why is it classified, why does it carry that particular classification. It is not too much more effort, at this point, to write down this rationale, so that other people can have the benefit of it. And it certainly makes the subsequent process, the subsequent dissemination much easier. People would realize what it is that they are really trying to protect. I would hope that by eliminating a great deal of what we now classify, that the total workload would be decreased.

But I think that by selecting our information, by knowing a little more precisely why we are classifying it, by reducing the total amount of information that we are going to protect, that we would end up with a security system that serves the interests of the United States better than the present one.

Remarks by Brig. General Delmar L. Crowson, USAF —

Contrary to my background — largely military — and contrary to the alleged conservatism attributed to the military, I don't intend to argue too strongly for the status quo. I do have a couple of practical suggestions which, I hope, would take into consideration most of the comments that have been made today as to how one might proceed.

Most of the suggestions I have result from my experience in a mixture of military organizations, a mixture of civilian-military, military-civilian, and finally civilian organizations. In each case, I faced classification pressures from many angles, and for different reasons.

I hold to the thesis that there is a need, as far as lifetimes are concerned — and even initially in the classification — for a more systematic and higher decision-level making arrangement in classification than is presently in existence.

In support of this, I am impressed with the constraints that are placed on the classification people, particularly by treaties — for instance, the Non-proliferation Treaty and the negotiating stance that we have to take in various kinds of operations like the SALT talks. Also, proprietary information needs to be protected — to protect the commercial interests of certain organizations.

In other words, the complexities of the problem of what interests are involved seem to me best served by understanding the constraints and mechanisms which affect the classification.

So, therefore, considering the restraints, considering the wide points of view that are represented by a classification decision, I argue strenuously that there is a need for a higher level, more systematic classification arrangement than: (a) is presently in existence; or (b) is contemplated.

I argue also strenuously for my second point, that as far as the need for a wider and higher level system of classification, there is also a need for a wider and higher level system for declassification or release of information, or the necessity for announcing policy when this happens. In other words, the reasons for convening a rather widespread group — and incidentally, I agree with the speakers that have been involved here on the fact that the problem is so immense that it appears to be impossible to attack on a general basis; reveal that it has got to be attacked on a case-by-case basis.

However, I would caution you that the interfaces of the problem and the sidewards looking arrangements that one has to have, as to the effects on others, must be brought to bear.

I believe that Jerry Kahan's suggestion that the military policy and political policy can be separated is probably true in such a mechanism.

However, I think that you are going to run into so many gray areas that it is going to be almost impossible for an individual or a group of individuals, who do not represent a very broad spectrum of the government, to get on with this.

I guess in closing my brief remarks here, I would like to say that I don't underestimate, in any sense of the word, the complexity and the seriousness with which classification and declassification has to be faced. There are many things at stake — and these many things should be taken into consideration at the highest and the most authoritative levels that one can get in the government.

I have one alternative which I recommend that you not take: That is, whatever you do, don't go to the couch and have your psychoanalyst or psychologist take over the problem. This will only create more problems than you have.

However, I believe that there is need for a systematic review, one, perhaps, that is done at key points. This has been suggested by a previous speaker. He suggested the points might be where hardware is revealed, or successive developments of hardware, or where policies need to be announced. I think we have to stick to the basic precept that classification, as far as lifetime is concerned, is like weather information. It is perishable. And if it isn't timely, and if it doesn't meet the requirements of the situation, you might as well not put it in the deep freeze, and you might as well not put it in the icebox, and you might as well just let it lay out on the drainboard to rot.

So I guess, as far as I am concerned, that decisions as to what you keep in the deep freeze, what you keep in the icebox, and what you let out on the drainboard to rot, has really got to be made at a higher level than it is being made at the present time.

Questions and Answers —

Workshop Leader Durham: I think that there were some interesting points that came out of this talk this morning:

Jerry had an interesting approach, basically one which categorized and maybe classified by functional areas. I could see some merit in this, having been in the business for a while.

Steve had a point that I have believed in for a long, long time, and it is not new with me. I learned the trade from Dr. Redman. And this is a statement of why something is classified. I personally don't have to live with the DD 254, but I have often thought that the DD 254 would be much more succinct if it contained the rationale of what it was. I think that this would be a great assistance to keep from over-classifying information.

I have to take the prerogative and ask Del the first question: How would you envision a higher level, and what is the forum that you see, Del, as a higher level, to what now exists?

General Crowson: I envision that you who are in the classification business, and who are the professionals, shall we say, with respect to interpretation, should have a very broad set of inputs to your deliberations. And I would view a higher level as being someone, for instance, like the Deputy Secretary of Defense; or, someone like the Commissioners or the Chairman of the AEC, as having a definite and a deliberate role to play in being able to hook up the political with the threat that is involved to the national security, and who is definitely responsible and answerable to both the President and to the Congress and to his own organization.

And all that I am saying is that it is time that the role of the classifier and the declassifier and the system that is involved has to be necessarily expanded to include the decision makers who are at the top and the decision makers who are at the bottom, so that the widest

possible set of inputs can be given to the deliberations.

The consequences — the evaluation of the net worth of what you are supposed to do or what you are doing — I think, has got to be made at a higher level than is being done now, despite the fact that classification guides get reviewed from top to bottom.

I think that we have got to focus on the point, and I think that we have got to have an organization to do it.

Mr. Charles V. Uhland: This is Charlie Uhland from General Electric in Philadelphia. I agree with you as far as the higher people deciding what and why to classify, but I think that the decision on how to classify, how to protect it, should be at a lower level.

I think that the people who are deciding how now are not acquainted with the problems down at our working level.

Workshop Leader Durham: Charlie, give a specific, would you?

Mr. Uhland: Well, if you were classifying the frequency of a circuit fuse or something like that — some electronic fuse or other — the fact that it needed classifying, and why it needed classifying, would be made upstairs, but down at the lower working level how to protect that information would be, for example, possibly the visual access to the window; possibly the casting that holds the window would be classified. That decision should be made down at the technical level, rather than by the people upstairs.

Workshop Leader Durham: All right, but let me say this:

If you took Dr. Lukasik's suggestion of saying what it is that is to be protected — would this not give the lower level . . .

Mr. Uhland: No. The people who make the decision on what and why aren't the technical people at the lower level who should decide how or what to protect, hardware-wise.

Workshop Leader Durham: Any other comment on Charlie's point?

Mr. Edward J. Reiss: Ed Reiss from the Army Material Command.

I subscribe to Charlie's thoughts. I have had an experience where the decision was made at the DA level to classify a program related to lasers. The letter of direction went directly from the DA level to AMC and the concept in handling this program would be comparable to handling TS information.

Apparently, it never occurred to the guy who developed the letter of directive to talk to somebody at the working level who has to deal with the matter.

If there is a coordination between the higher DD level and a working echelon, you could come out with a better program.

General Crowson: Without a very close relationship between what the guide says, for instance, and what the physical security setup is, I think that you have got an unworkable system.

Mr. Di Peri: I made a proposal some time ago to have a Division of Technical Security within the Office of Classification Management, and the function of this Division of Technical Security — at least, the proposed function — was to have highly qualified technical people across the board, generally scientifically qualified, to be stationed in various regions of DCAS or what are now DCAS, to assist in making these technical decisions at the contractor level. It would be a sort of a liaison between DD and the industrial contractor, and he would be a technically qualified person who could go in and talk to the engineers, and make realistic guidance suggestions on the implementation of the requirements of DD 254.

Of course, that has never come into

being. It may some day become a reality. I hope it does.

But that would solve some of the problems inherent in this communication between DD and the contractors, who basically have the responsibility for generating a lot of information that has been, well, derivative classification. They have been required to classify certain information, and now DD wants to make sure that it is being done properly. These people would be the coordinating activity between the two.

This is one suggestion anyway. It has been available for a long time.

Workshop Leader Durham: Steve, do you want to comment on that, since you are the DD rep?

Dr. Lukasik: Well, I certainly agree that anything that makes the operation of the system more rational is greatly to be desired.

I think that it is true that there isn't enough interplay between the people who make out security forms and the people who set overall policy and the people who do working level classification and the people who have to protect the information.

I think that is an organizational problem of no mean magnitude because it spans so many levels and so many organizations, but I think that there is no doubt, you know, that someone has to do something like that, or else the system will just continue to accumulate defects and be subject to abuse.

Workshop Leader Durham: Steve, is Dr. Foster's proposed technical review at key points a step in this direction?

Dr. Lukasik: I think that will help, too, because it will focus attention on:

(a) The specifics of the program — that is, on a program-by-program basis, and

(b) It will force you to think about the subject matter, rather than just some general thing like: "Well, that is a strategic capability" or "that is a vulnerability" or "that is related to nuclear weapons" or something like that.

So, I think that both of those are good steps. However, I think that the sort of thing that we were all talking about this morning suggests — and even have brought up in the course of these questions — suggests an even deeper penetration into the "innards" of the system.

Mr. Roy L. Wesley: Roy Wesley, Grumman Aerospace. A question for you, General. You pose the need of a higher review. Can you give us any information as to what is the likelihood of this need being satisfied at a higher level? You state that there is a requirement, but is there anything actually happening in the government so that we down in industry could have a better direction and maybe solve some of these problems?

General Crowson: I can't tell you specifically what is going on within the Government. There are reviews, obviously, that are taking place as a result of certain revelations that have appeared in papers and magazines to be unnamed.

Mr. Wesley: Which we all know!

General Crowson: Shall I say, I won't mention the name, but they are initials of the New York Times.

From where I sit in the Atomic Energy Commission, I don't have a classification problem basically. I have a big physical security problem. And I have had to look at the problem from the point of view of protecting literally unclassified materials in the interests of national defense and security — which is a real anomaly in your business. Consequently, I have grown to feel over the last three or four years that one can't really have a consistent policy between classified

information and unclassified information as far as the national defense and security are concerned.

My theory really comes from a point of view of frustration. I wish that somebody at a high level would take a view of it.

Mr. Kahan: May I just ask, General Crowson, if I may, about this anomaly that you pointed to when we were discussing the question of over-classification — the anomaly that you raised of a need to protect, through physical security means, information that is not literally classified. Could you explain even in general terms what that problem is? What is the authority on which the U.S. Government could take such action?

General Crowson: Well, this is germane to the problem.

Workshop Leader Durham: It is an interesting case. Do you want to expound on this thesis for a second?

OK, let me just say what we are talking about — and you can correct me if I am wrong. This is the nuclear material problem. General Crowson is responsible for the "protection" of nuclear material.

From the Floor: I thought this was for official use only.

Workshop Leader Durham: No, that is not what he is talking about. No, over at Atomic Energy, he has got to account for all of the fissionable materials that this country has got.

General Crowson: Unfortunately.

Mr. Kahan: Well, that is really outside the classification system.

Workshop Leader Durham: Yes, that is really atomic energy.

General Crowson: Let me make a brief comment about it:

The anomaly arises as follows: that plutonium is a material that has not only strategic value for bomb purposes, but also for reactor purposes, for peaceful uses. The material plutonium, as such, in its isotopic content, when it is just plutonium, is unclassified. There are materials such as plutonium in all of its isotopic contents that appear on both the classified side of the weapons program, as well as on the unclassified reactor side of the program — the material having had national defense and security interests because a little of it goes a long ways.

To put it, I think, in those terms, the important thing is then, how does one insure that the material that one has, either in the defense side, the AEC side, or the civilian side, is not being diverted to "uses that are unauthorized" such as making of bombs clandestinely from unclassified materials.

So the anomaly really arises from the fact that one can protect unclassified materials through the imposition of security arrangements, but the law does not permit, at the present time, the invoking of "formal security arrangements" with respect to unclassified materials.

So what we have to do is to seek the authority from the Congress to change the Atomic Energy Act, which would grant the necessary authority to the Atomic Energy Commission to invoke or, shall we say, in the national interests, to put out a classification — not classification, but prescribe physical security measures that would be applicable, including security clearances, perhaps, or background checks of some type, some sort of indices that would permit one to evaluate the risks that one is taking when one puts this material into commerce.

Now, this is where the anomaly arises. And it is something that arises not only in the reactor business, but also when you introduce the material into the transportation cycle, where it literally disappears out of "physical control" of a plant and goes in as an article of commerce into the transportation cycle. You can imagine the consternation that one has when the

material doesn't arrive on time.

Mr. Robert E. Neal: I am Bob Neal from TRW. I would like to direct a question to Dr. Lukasik:

How do you feel about making decisions at your level within, say as to the state of the art, basing classification or declassification on that?

With tne engineering people in my company, this is a thing that I hear a lot of the time: "I have to classify this, and this is 'horse and buggy' in the state of the art. There is nothing unique about it; it is a common engineering technique that everybody knows, or a principle that everybody knows, and if you are going to do this thing or build this thing, this is the way you do it. But still we are classifying it."

Dr. Lukasik: Are you thinking in terms of assessing our state of the art or the adversary's state of the art?

Mr. Neal: Our state of the art, or the adversary's, whichever way you want to go.

Dr. Lukasik: Well, I will just make two observations:

One is that it is very common for our technical people to, of course, get so used to something that they get the feeling that any idiot knows that, and so there is a tendency to underestimate the value of some knowledge, or a technique, or a capability, just due to familiarity. And I think that one must be aware of that.

Now, if one is classifying Fourier integrals, that is sort of silly. But, on the other hand, there might be some techniques — manufacturing techniques or theoretical approaches that might well be protected above and beyond the point that the garden variety of user may think that it is worth.

On the matter of assessing the adversary's state of the art, that is clearly a lot more difficult. And sometimes you go to the intelligence community and you do get very good information out of them, or at least enough to satisfy you that you can make a decision.

Other times, of course, the intelligence community must admit that either they don't have very good information, or once you look at it, you come to the conclusion that it is not adequate for you to make a decision. So that is probably the much more difficult case.

And I think that in a case like that, in view of the importance of national security, prudence tends to make you come down on the conservative side.

So, I think that those are probably the two factors. I think that in some sense, the higher the level, the easier the decision becomes because, in fact, you integrate a lot of trains of thought, and a lot of information. On the other hand, I recognize the fact that at some height, you can completely lose track of all the problems that your decision implies.

I don't that that is an enormously difficult problem, although I will admit that there are cases where you simply will be unable to make the decision on the other side's capability.

Mr. Di Peri: I am reminded of something that was said earlier — this gentleman on the end said earlier that if we have information upon which decisions must be made, the people should be given all of the information so that they can make decisions. It came out something like this: We should release more information so that an informed public could make a decision.

Dr. Lukasik just pointed out that the intelligence data that is available sometimes leads to very solid decisions that the enemy's state of the art is at such and such a stage. However, there are times when he gets intelligence information that gives

him a pretty good guess figure. And he can roughly estimate, but he is not sure.

Now, if this kind of information was presented as a fact to the public, knowing that it is very, very shaky information, couldn't the public come up with the wrong slant?

Mr. Kahan: I think that is a good question, and the way I would answer it is this:

I think that when the Executive Branch is unsure, is uncertain and still must make a decision, an important national security decision, in the face of those uncertainties (and a non-decision is also a decision), then if it is crucial, the public has a right to know that, in fact, the Executive Branch is not fully aware of which way the adversary might go.

Otherwise, what you do get by inference is, to use an example, the public impression that, in fact, our land-based missiles are going to be knocked out tomorrow; because, by not explaining adequately enough that we weren't really sure whether that could happen, but still at the same time going ahead and arguing strongly for the Safeguard ABM to defend those missiles, the public got the impression that the threat was right around the corner. Being more candid about the fact that we weren't sure, and then arguing the prudence line, if that, in fact, was what it was, the public could react and say: "we think that is excessive prudence" or "we support your prudence."

Mr. Di Peri: Well, the thing is, doesn't prudence also dictate that if you are not sure and the enemy doesn't know whether you are sure or not?

Mr. Kahan: I agree.

Mr. Di Peri: That you should not let it be known that you don't know?

Mr. Kahan: That is the trade-off I spoke about.

Mr. Di Peri: I don't think there is any trade-off, frankly.

Mr. Kahan: Well, I think that it depends upon what and how much detail. I would argue in many instances that I would side on the side of safety but in other cases I wouldn't.

Mr. Di Peri: It is a case-by-case basis.

Mr. Kahan: Yes.

Mr. Di Peri: Not general guidance.

Dr. Lukasik: There is another point here on the matter of when the Executive has some degree of uncertainty.

You say, well, why don't we just sort of present the case, as it were, and then let a broader group make up its mind.

Well, first of all, there is the obvious problem that you now start to run into the disclosure of intelligence information, which gets you wrapped around the axle on the question of protecting sources.

But the other point, too, is — if I may be excused a certain degree of the inevitable executive arrogance — if a group of people who have made their career, as it were, on studying that particular problem can't make up their minds, it is unlikely that the broad publication of all of the relevant documents and argument by a broader group of people is unlikely to come out with the truth.

I think that it is important, however, as Jerry would say, to first of all, announce when you are making these decisions and give some indication of the firmness with which you stand behind that; because the trouble is, there are some things that we, in fact, do know very well, and we ought to do probably exactly what we are doing. And there are other times when one is relying more on the prudence, or the uncertainty, or the work case, or insurance, or hedging one's bets. Whatever nomenclature you use in those situations, I think that we sometimes,

in fact, tend to present the case, perhaps, more strongly, or very strongly, on what really turns out to be weak, or ambiguous, or non-relevant.

Mr. Robert L. Taylor: I am Bob Taylor from Indiana University.

Dr. Lukasik referred to something that I would like to challenge you on here. With regard to scientific and technical information, it seems to me that Bower's report on second order consequences would identify for us something that we have to look at, and that is that you would take a group of scientists and technologists who were, let us say, the so-called "invisible college" for that particular discipline, and say that they were best at deciding which should be classified and which should not be. Yet the second order consequences, i.e., ecological consequences, that they could not determine at that time would have to be looked at by another group that you would possibly exclude because they didn't have the right to know that particular information regarding that particular discipline.

There are two other assumptions that I would like to bring out now that I would like to challenge:

You said before that behavioral theory really didn't offer anything for proving that a free flow of scientific and technological information was best. But I asked about Marsh and Simon's postulants in the book, Organizations, where they take a number of questions relating to concepts in problem solving and through empirical research, by Bablos and Barrett and others in communications theory, have shown that the nondirected small groups where there wasn't a filtering of information by any one person or control of information proved to get better results, particularly in the area of solving creative problems, which, I think, could be related to our R&D environment that we are talking about.

So, I think that there is some theory that can be drawn upon — and as a matter of fact, there are a number of studies going on now at MIT which are testing this free flow of scientific and technological information — notably by Thomas J. Allen.

The third thing is that I think that it is very unfair to compare the Soviet's closed system and our system with regard to the effect of closed and open information flows because we are, in effect, comparing two different internal systems.

Theirs is much more centralized than ours, and they don't have the problems of two people — one in Los Angeles and one in Long Island — working on the same problem and yet not being able to know about information that is going on, because of the restriction of information.

So those are the three things that I would like to challenge your statements on.

Dr. Lukasik: All right, taking them one by one:

The security versus the college, I think, is a very, very interesting question, a very significant one. I think that there is probably not quite as much of a problem there because usually the information required for the ecological judgments — like what is the yield, or what is the altitude, or what is the depth, or what is the location — generally is not a problem to protect or else can be dealt with sufficiently parametrically that national security can be protected without giving away the specifics.

So, I think that that raises a problem, but I think one that rational people can work out. I don't see any inherent conflict between security and, say, ecological concerns — or any other; you know, there are other areas of public interest besides the environment where conflicts occur, but at least in this I don't see it.

So I don't see that as terribly crucial, except that you have to handle it intelligently. The numbers in

security are often very important: What is the yield? What is the altitude? What is the frequency? On the other hand, with the ecological problems it doesn't make much difference whether it is one megaton or ten megatons — it either is an important effect or it isn't and there are usually few critical thresholds which requires you to know precisely what the number is. And that is, I think, the region within which you can maneuver and get your answers, and at the same time protect security interests.

On the question of the role that behavioral theory plays, it is probably, in some sense, a statement of the hard scientist versus the soft scientist.

From the experiments that I have seen and what I have read and heard from people in the area, I think that there is still quite a gap between the insights, the laboratory experiments, the sophistication of the models, and the insights that one gets, and their applicability to the real world situations.

Having lived within the real world situations and having seen how the bureaucracy operates, I think that it is incredibly richer than the kind of models that tend to be dealt with, either mathematically or experimentally, in these things. But I will admit to a certain amount of the hard scientist's prejudice.

On the case of the United States open system and the Soviet closed system, admittedly it is a difficult comparison because we don't live in their system, and one should to really make the comparison precisely and fairly and accurately. I think that what you are saying is that one should know as much about the "innards" of their system and how it operates as one knows about the "innards" of our system and how it operates. I agree with you completely. I think, though, again when you look at data and draw a conclusion, you also have to do a sensitivity analysis; and you say well now, let me wiggle all of the parameters or premises that went into my conclusion to see whether it would change drastically, if one of them was a bit wrong.

And I am speaking intuitively, but I do have the feeling that — having done that kind of a sensitivity analysis — that the conclusion is still right. That is, I don't think that if I were embedded in their system that I would come to any different conclusion — that is, that their system is a closed system with a great deal of internal constraint, and it seems to operate quite effectively, you know, in terms of output.

I mean, roughly the same inputs give roughly the same outputs, and they are, obviously, a capable adversary and yet they do have a different way of going about it.

Mr. William G. Florence: Bill Florence, Consultant. Dr. Lukasik, last year the Director of Defense Research and Development urged that R&D information which could qualify for security protection under very strict criteria be held under secrecy for no more than two years as a general rule.

Is this still the view of the DDRD today?

Dr. Lukasik: I must confess that I haven't talked to Dr. Foster on this specific issue since, in fact, the time period that you are referring to, so I would like to beg ignorance.

I did, however, in my remarks, address the question of lifetimes and made the point that — or led up to this case-by-case approach that says that there are some times when longer lifetimes are quite reasonable, and I would argue, justifiable, and there are other times when the shorter lifetimes are appropriate.

I really would not like to argue the one-year or two-year or five-year kind of thing, because I just haven't looked at enough data to have a firm opinion. Some people have come up with those numbers, and I am prepared

to defer to their judgment.

Mr. Florence: Mr. Durham, I will ask another question then, and this will be to General Crowson:

I am very much interested in his proposition that we should change our present practices to provide for a high level decision for imposing security requirements on information in connection with programs or matters of interest. I have been supporting that theory as long as I can remember.

Now assuming that we do make changes this year or as shortly as we can in this Government on our present classification system and we do allocate to a higher, a much higher level, decisions that really impose security restrictions on our information, then this question arises:

The high-level man is not going to be too much concerned with detail, like confidential or secret. He is going to be concerned mostly with whether or not disclosure of the information involved would actually create a real defense problem for us.

So I would like to open the question for discussion of whether or not we can get along with one so-called security classification, or whether we need more than one, in this type of decision that we are speaking of?

General Crowson: Well, I certainly agree with your analysis of some of the benefits and perhaps one of the major drawbacks that you have briefly touched on is the fact that the gradation of the system right now is rather imprecise. Perhaps the suggestion that we consider everything on a case-by-case basis might lead the decision makers to a point where there is information that, if revealed, is detrimental to the United States; whether it is political information, whether it is strategic plans, whether it is different kinds of vulnerabilities that various weapon systems possess, or similarly that there is material for sale somewhere in the world that is inimical to the U.S. interests — there may be one classification — for national defense interests.

And consequently, you might do away with all of your present gradations from "Official Use Only" on up through "Top Secret," because basically that is a system that was put together to compartmentalize the information.

And one of the things that I think we are arguing for is that compartmentalization is basically a damage-limiting strategy.

Someone said, the problem with democracy is that it is the only ship — that is the "ship of state" — that leaks from the top! If you stop the inadvertent leaks, if you can stop the purposeful leaks, or the trial balloons, perhaps you can get part of the way to where Jerry wants to go; but, as I say, the suggestion is certainly not unreal.

Mr. Kahan: On the point of leaks and trial balloons, I think that the fact that there is such a thing as official leaks or background leaks, says something about the Executive Branch's own interest in circumventing its own system for, probably, very sound reasons — getting the public apprised, sensing broad domestic reaction to a policy, and even testing international reaction to a policy, let us say.

And I think that it is interesting to note that if the Executive Branch tries to circumvent its own system, that maybe we should, in some sense, make it easier for the Executive Branch to do what it seems to be trying to do in a more legitimate way by loosening its own system and letting it be known that everybody agrees that there should be some kinds of decisions and information which it should very forthrightly put out — in fact, that is what we have been talking about here.

And so I would, of course, not oppose the continuation of official leaks or trial balloons for these reasons. There is a limitation to how much comes out in these official and other leaks because the Executive Branch is

still uncertain as to how far it wants to go, or how far the American people want it to go, and how far it can safely go. You have to rely on inadvertent leaks to get the full body of information. Replace the inadvertent leaks — the cynics who are trying to pull the Executive Branch down. I would rather replace those people with an official recommendation. It is hard to rely on people who want to breach officialdom with perhaps misguided attempts to increase information.

But as you open up the Executive Branch officially, I think that, willy-nilly, you will probably reduce the number of inadvertent leaks, because you will get more official information out — and ultimately, that might be better.

Mr. Thomas: Yes, I tend to agree with everything that Jerry said.

I was going to address myself back to the question about the number of categories of classifications. I think, operationally, the main difference, let us say, between "Confidential" and "Secret" and "Top Secret" is how much of a background you do on the people. Everybody who handles classified information has to have a background investigation and get a "Top Secret" clearance; and that, it turns out, proves to be a very expensive way. Short of that, you probably must necessarily have some other, you know, classifications down the line, and I am not prepared to argue whether the number should be two, three, four, or five. But it strikes me that the present number isn't unreasonable in this area.

General Crowson: Perhaps not optimum.

Mr. Thomas: It may not be optimum; I hadn't thought about it very much.

* * * * *

WORKSHOP B — SECURITY COSTING IN RELATION TO CLASSIFICATION

Remarks by Workshop Leader Robert E. Green —

It is usually hazardous, I think, for any speaker to assume that some basic premise that he may make before a large audience is going to be agreed upon by that audience. However, before this group I am confident that we are in agreement on the fact that security classification and the handling requirements that it imposes has significant cost implications which must be identified and minimized through thoughtful and knowledgeable classification of information. The very existence of the Classification Management Program may, in fact, depend on our ability to demonstrate that good classification management results in cost reduction and cost avoidance.

I am reminded of a debate I had a while back with the Director of one of the Navy Laboratories. A temporary impasse was reached when he declared that he would devote no manpower to a Classification Management Program until savings in his Laboratory programs could be identified and proved. My answer to him was that that would not likely occur until some resources were devoted to the task. It was sort of a chicken-and-egg situation.

But, from a pure management point of view, it is understandable that the highest priorities go to those administrative programs which produce realistic and identifiable savings. It is not surprising to note that every Seminar conducted by NCMS in its brief but significant history has addressed the subject of security costs.

Here is a quote:

> A panelist on this subject should ideally have — good, solid figures on actual savings, achieved in real-life situations in classification management — thereby benefiting the national defense and winning appropriate plaudits for himself from Top Management.

> In trying to assemble some information on savings, I have come to realize that the reason it is scarce is simply that we don't yet have a body of information on the costs of classification.
>
> If you don't know costs you just can't talk about savings in satisfactory terms.
>
> Worse, if you don't know costs you can't really make intelligent judgments about whether given controls or protective measures resulting from classification are worthwhile.
>
> It therefore seems imperative, if we are going to improve our classification management, to acquire a body of information on costs.

If those words sound familiar, you may have been present at the very first NCMS Seminar in July, 1965, when they were delivered by a panelist on the subject of realizing savings from classification management. The same thoughts have been expressed in various ways each year since.

In presenting this panel, it is our objective to analyze some identifiable security costs, to determine how they are influenced by classification assignments and how they might be reduced or avoided with little or no loss of security. We hope also that these discussions will tell us whether any progress has been made and what course of action we should now pursue.

It was decided from the outset that we would not attempt to identify the cost of making a classification determination. The variables in this process are so great that figures could only be developed on a case basis and would not be applicable elsewhere.

We will instead address three specific areas wherein some uniformity exists and where some prospect of developing norms exists. They are:

— Packaging and transporation of classified material.

— Establishing and operating a closed production line.

— And, the costs of document handling — the so-called overhead or administrative costs.

Remarks by John F. Pellant —

This has to do with the securing costing related to shipping, and this presentation deals with two interrelated but separate disciplines in the logistics area — transportation and packaging.

Transportation has sometimes been referred to as the "Achilles Heel" of security. This is relatively understandable, because material moves through an environment which does not lend itself to those specific controls normally available at a fixed facility; freight is normally handled many times by many people under all types of conditions, thereby giving the appearance of vulnerability.

First of all, a carrier accepts custody of freight under a contract of carriage. He is enjoined by statute to transport the freight to the consignee safely and efficiently. If he does not, he is liable for losses or damages that may occur. No transportation system has been devised which will guarantee 100 percent effectiveness just as we ourselves are not 100 percent sure of what will happen tomorrow or what will happen in the next ten minutes. However, to obtain the maximum assurance of success, transportation systems have instituted a series of safeguarding measures as a normal practice to reduce the incidence of loss and damage.

Material when received by a carrier is tallied and receipted for on a bill of lading. If the material is taken to a carrier's terminal for consolidation with other freight, the lading is tallied upon unloading and is retallied upon reloading for outbound movement. If the material is not

taken to a terminal for consolidation but is transported direct to the consignee, the tally is performed during unloading and is verified by the consignee. Now this tally relates to the package being shipped — not to the contents thereof. Please remember this point because it is very important in the transportation cycle.

Tally of the package places emphasis on the package or shipping container. Good packaging is designed to protect the commodity from damage during the handling/transportation cycle. Good packaging is also used as a deterrent to pilferage. No one who is security-conscious would challenge the general premise that good packaging is also a deterrent to compromise.

Now comes the rub — identification of costs — how much can be spent to achieve a package that will minimize the possibility of compromise? Converting a good transportation container into a security container could easily increase packing costs tenfold. A 60¢ box could easily cost $6, and one-hundred boxes means an added expenditure of $540.

Now, what is gained thereby? Usually, a good container does not break open in transit; usually neither does the security container. The security container will deny more time to the intruder — but — it will not deny access. The good container, used as a normal practice, for a particular commodity is noted normally as an item of freight and tally; a security container used for the same commodity immediately invites attention because it is not normal.

We will not dwell on motivation, objectives or reasons for pilferage, except to make a basic assumption that the nature of the intrusion is that of:

(a) Selective access, and/or
(b) Random access.

In dealing with the security of classified hardware, we are almost totally concerned with "selective access." Somebody wants this piece of material.

Normal good packaging and normal contract of carriage procedures are usual procedures initiated to transport freight safely and reduce or eliminate loss and damage payments by the carrier.

Whenever containers are changed for additional deterrence, that is, four or two way strapping with seals where not normally required; noun names or markings omitted when such marks appear on all other nearby containers; more expensive box styles in lieu of those normally required for the commodity shipped; or, there is an obvious imbalance between net and gross weight stenciled on the packages — we are assisting the selective intruder in his search for his object.

In like manner, in compliance with DoD Directive 5200.1 when we require signature tally and service, locked and bolted vehicles, or impose peculiar control procedures on the transportation industry we are also assisting the selective intruder to find his object. We have thereby defeated the best protection available in transportation and packaging — and that is the anonymity of a package among myriads of similar packages within an industry whose prime purpose is to transport packages without loss or damage, realizing a profit therefrom and maintaining its business thereby.

In this area, it is interesting to note that the DOT, the Department of Transportation, and the Transport Association of America had a conference on cargo security crisis, and representatives of retail, import, and labor observed that markings and extraordinary packaging procedures tended to assist the random pilferer to select a more important target.

Also, the advent of large locked containers and containerization programs have given rise to a different type of pilferage — organized. Now

instead of taking a case of shoes, they merely hijack the container with a whole load of shoes.

The additional service required of the carrier industry must be requested at the time of movement; this action alerts the world at large to the movement, making interception and intrusion easier. If an intruder really desires to acquire a particular piece of material, steps can be taken to accomplish this purpose regardless of the controls imposed.

The increased requirements placed on the shipper by DoD Directive 5200.1 in essence requires that in the absence of government capability or because the commodity characteristics require commercial carriage, Confidential shipments will be made under signature service and Secret shipments will be made by authorized (that is, industrially cleared) carriers or under escort. Now again we have the cost problem.

There are no figures available as to the number of shipments, the weight per shipment, etc., pertaining to classified material, nor can we equate actual losses, compromise or suspected compromise. But we can get a feel for costs in the area of loss and damage for surface transportation by using simple class rate and distance averages for the movement of general commodities weighing 100, 1,000, 5,000, 10,000 and 24,000 pounds, respectively:

If we are moving a 100-pound piece of material, a general commodity that is unclassified, the cost will average about $10. If we impose signature service for "Confidential" on that same piece of material, our costs become $40. If, however, it is a "Secret" and we have to use a cleared carrier to move it, our costs to move that 100-pound object now becomes $2,040. If we use a carrier who is not cleared and must have a carrier escort, our costs are now $3,080. If we use a government escort, we reduce the cost somewhat to $2,510. If we go out and rent a vehicle to move the 100-pound piece and move it ourselves, it is $800.

This cost is common to the whole segment of weight loads, and we will take as an illustration, 24,000 pounds of general commodities:

Unclassified will cost us $750.

Confidential is $780.

Going to the Secret area comes to $2,040 — the same figure that it would cost us to move the hundred-pound box.

I must mention here that in the absence of signature service for the carrier industry, you then escalate the security protective procedure to that of "Secret," so that if no carrier will provide you signature service for the 100 pounds, you will automatically jump to the 2,000-pound level to move a piece of material.

Now, if we deal with A and B explosives, we have a little different picture. We will take the movement from Doyline, Louisiana to Concord, California as a specific example:

One-hundred pounds of class A or B explosives would cost you about $250 unclassified, $290 classified "Confidential," $750 classified "Secret" by a cleared carrier, $2,250 by an uncleared carrier with escort, $1,050 for an uncleared carrier with government escort — and again $800 by leased or rented vehicle.

A 30,000-pound shipment of A and B explosives will cost you $3,150 normally, $3,180 "Confidential" and signature service, $3,640 for a cleared carrier, $5,230 for an uncleared carrier with commercial escort, and $3,950 with a government escort — and again $1,310 for a leased or rented vehicle. The reason for the difference, of course, in the leased or rented vehicle, you have got a larger vehicle and it will cost you more money.

Now these figures are available in this handout, and these comparisons

do not take into consideration cost trade offs in movement by different modes of transportation, because that is a traffic management determination to be made depending upon the circumstances of movement at the time it transpires.

But these are the relationships of surface transportation.

To arrive at some conclusions or patterns related to pilferage, we can look at loss and damage in the carrier environment. In the rail system, freight claims paid for theft and/or pilferage amounted to 2.4 percent of the total claims paid in 1970. Now most claims were paid covering household goods or products, foodstuffs, motor vehicles, tobacco and spirits. Commodities such as machinery, metal products, etc., among which most classified material would be found, constitute about 1.5 percent of this total theft or pilferage factor. A similar pattern exists in the motor carrier and air industry.

Within Navy, nondelivered supplies (which include items ordered but shipped only in part or not shipped) indicate that commodities which lend themselves to possible security classification, such as electronics, ordnance repair, aeronautical repair, products, and so on, make up .003 percent of the total dollar value of nondelivered material.

This constant pattern indicates that pilferage and theft are related to common usable articles which are easily disposed. The pattern also indicated that such material is readily recognizable in the transportation systems by marked peculiarities in packaging, conveyance or control.

I have usually been in the chain of investigation on possible compromise of material lost in the transportation system, and since 1957 I have had not more than a dozen different files cross my desk, and in no case was a compromise a proven fact in these cases that were brought to my attention.

Now when we compare general commodities and explosives, all of the foregoing safeguards that were mentioned before — the tally, and so on — apply to commodities other than class A and B explosives. Now there are additional safeguards placed on packaging and transportation of explosives by statute. Any carrier transporting explosives must comply with the hazard regulations promulgated by land, sea and air authorities.

Besides the normal tally count and documentation procedures applicable to general commodities, vehicles transporting explosives cannot be parked or sided in the same area as general freight; they must be held in a secure, guarded area. Carloads cannot be opened except in emergency and, in the case of defense shipments, immediate notification must be given to the cognizant command, if the seals are broken and the car must be opened.

Changes in DOT (Department of Transportation) regulations require drivers to inspect transporting vehicles periodically while in transit. This inspection is to ascertain the safety of the cargo and vehicle, but it inherently provides additional security.

To obtain economic advantages, the transportation industry constantly follows a procedure of tally checking to isolate damage and pilferage and insure service to customers. Safe handling practices are constantly invoked to reduce claims. Packages are designed to contain the commodity against handling and transportation damage. When commodities, such as explosives, are hazardous to the general public, regulations are imposed on both the shipper and carrier to reduce the incident of hazard. All of these precautions are followed when transporting freight without regard to the security classification.

You will remember that we mentioned before that carriers tally packages and/or conveyances — not the contents thereof. Shippers are required by statute to describe the freight shipped in freight nomenclature —

not manufacturing, cataloging or technical terms; carriers are obliged by statute to impose reasonable rates for carriage based on these descriptions.

The freight description for commodities cover over 10,000 items which embrace millions of articles of technical description. A classified item which is a part of an exotic piece of military equipment, if mechanical, is usually described in the freight systems as machine parts which is the same description used for non-classified mechanical parts. Unless specifically brought to the attention of the carrier, there is no way to isolate a package of machine parts which may be classified from other packages of machine parts which are unclassified.

Based on the foregoing, we have some recommendations:

It is recommended that basic security regulations governing the commercial transportation of classified material be revised to take advantage of the unique characteristics of the transportation and packaging systems.

It is recommended that such revision consider the separation of material into two areas:

(1) Hardware, the equipment itself, and,
(2) Software, the printed matter, blueprints, etc.

It may be possible to declassify some hardware for transportation purposes, whereas software perhaps should be more stringently controlled. This is quite obvious to you gentlemen because software can be reproduced very simply by cameras or other methods without actually divulging that compromise has been obtained.

In any event, it is recommended that just as classification experts should be consulted before assignment of a security classification, so also should transportation experts be consulted to determine the capability and possibility of maintaining security during that "Achilles heel" — transportation. Trade offs at the beginning should minimize subsequent classification problems, provide a concrete costing base and obtain more support to the end user.

Workshop Leader Green: I think a most interesting and significant aspect of this presentation is the fact that this extremely low loss rate — less than 3/1,000 of 1 percent of dollar values in commodity categories which would likely include the bulk of classified material being shipped. Bear in mind that not all of that 3/1,000 of 1 percent would be classified; there is some infinitesimal figure in that which represents the classified losses: 3/1,000 of 1 percent.

I think this factor might indicate that there are security features inherent in the transportation system which we are not fully exploiting, while paying premium shipping rates for special handling which affords very little additional security.

I doubt if many of us have given any consideration to the inherent security value in the anonymity of a shipment. Our efforts to increase security by exotic packaging, bands, seals, etc., could actually be self-defeating by calling attention to the special nature of the shipment. It is an intriguing concept and one, I think, that should be explored thoroughly and very seriously.

Remarks by James A. Buckland —

Whenever it becomes necessary for a defense contractor to establish, operate and maintain a closed or controlled production area, there will be cost increases in the operation, construction, and the maintenance of the production line. These costs can be both direct and indirect. Among them are:

a. The cost of construction of perimeter walls for a closed or restricted area production line in compliance with Section IV and Appendix IV and V of the Department of Defense Industrial Security Manual.

b. Costs both direct and indirect resulting from the needs for security clearances of various degrees for the production workers.

c. The cost of duplicating equipment and supply lines and supply sources together with operational inconveniences which effect production control principals and operations.

d. The cost of controlling the areas, hardware, equipment, and personnel as required by the Department of Defense Industrial Security Manual or much more simply security and accountability controls.

Today, we will examine some of these expenses and then through classification management action eliminate or reduce them. Most of us here are aware that whenever the principles of classification management are clearly, efficiently, and effectively applied to a given program or contract, the cost of the program for the production of classified information can usually be significantly reduced by both government and industry. This very definitely applies to the operation of closed production lines. Effective classification management may not eliminate the need for controlled production lines, but it certainly can reduce the size of the area, or the scope of the operation, and consequently the related costs.

When a defense contract is received for the production of classified hardware, there are several basic questions which must be considered:

a. Can the classified hardware be properly stored in safes, cabinets, or other authorized storage containers during nonworking hours?

b. Is the hardware classified TOP SECRET or does it require special controls or special access permits or other restrictions?

c. Is visual or aural access involved?

Once these questions are answered, many problems can be solved immediately. If the material can be appropriately stored during nonworking hours, the construction, guard, alarm, and supplemental control costs of the closed area are greatly reduced. However, if open storage of material during nonworking hours is required, area construction costs are increased. These costs remain relatively constant for all classified levels. Costs for guards and supplemental controls rise significantly with increased levels of classification and special access requirements. Visual and aural access also have a significant effect on costs insofar as the use of opaque walls and sound retardent walls are concerned.

These charts are basic plans for a closed production area indicating the cost and security requirements for the area. The figures are estimates which apply to our New Hampshire area and are based on optimum construction conditions. These are basic figures which we can use to indicate cost reductions.

Figure 1 is a proposed drawing of a closed production area. It is 75 feet wide and 150 feet long. Please examine the charts for the construction specifications. In this area visual access is a problem, aural access is not. All materials used in the construction of this room comply with the Industrial Manual. This area is built for the production of hardware of any degree of classification. However, if the hardware is TOP SECRET, it will be necessary to establish a minimum of one 24-hour guard post.

Figure 2 shows the cost of both material and labor for all of the construction of this room. In the right hand column of the chart, I have indicated the choice of construction for this area. Walls cost $20.50 per linear foot or a total of $6,150. Other costs shown are for the screen-

CLOSED PRODUCTION AREA

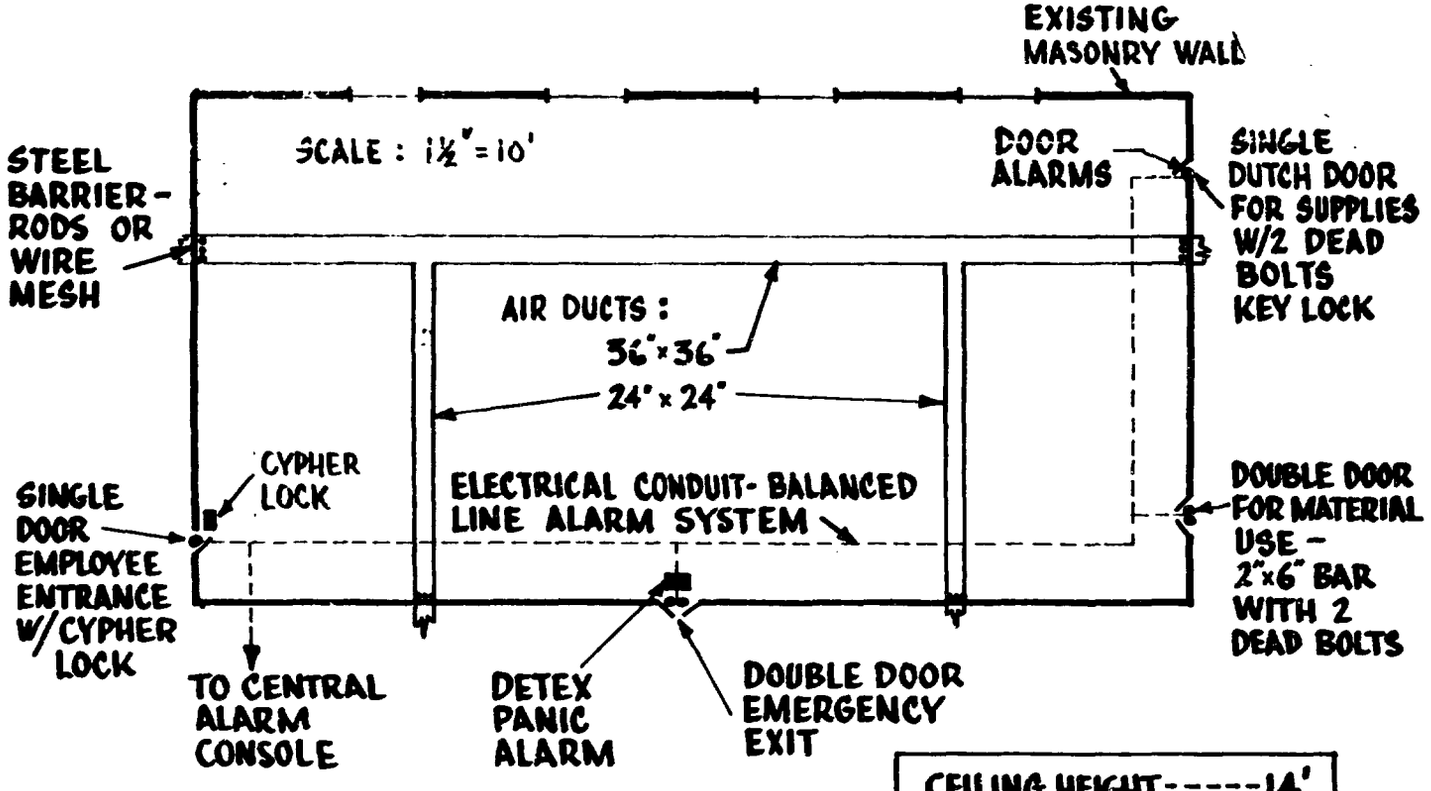


Figure 1

CLOSED AREA CONSTRUCTION COSTS

TYPE	MAT'L	LABOR	LINEAL FT TOTAL COST	MAIN AREA (CHART #1) LINEAL FT	MAIN AREA (CHART #1) TOTAL COST	REVISED AREA (CHART #6) LINEAL FT	REVISED AREA (CHART #6) TOTAL COST
WALLBOARD, 2 SIDES, HOLLOW	11.00	7.50	18.50	300	5550.00	180	3330.00
WALLBOARD, 2 SIDES, FILLED	12.00	8.50	20.00		6150.00		3690.00
WALLBOARD, 10' w/24" METAL FLOOR LOUVRES & 24" WIRE CEILING VENT	13.00	7.50	20.50		6150.00 6150.00		3690.00 3690.00
MOVABLE PARTITION-7' w/WIRE TO CEILING & 1' VISUAL BARRIER OVER PARTITION	10.50	4.00	14.50		4350.00		2610.00
WIRE MESH FLOOR TO CEILING	9.00	16.50	15.50	300	4650.00 (1500.00 SAVINGS FOR EXT. VIEW		2790.00
WINDOW BARRIER:				SQ FT	TOTAL COST		
WIRE SCREEN PER SQ.FT.	.65	.25	.88/SQ.FT.	384	337.92 337.92	96	84.48 84.48
ENTRANCE (DOOR COSTS) PER DOOR:				TOTAL UNITS	TOTAL COST		
HINGE PER TAPPING	.15	6.50	6.65	7-HINGE ST	46.55	5-HINGE ST	33.25
WOODEN BAR w/ BRACKETS	2.00	6.50	8.50	1-BAR	8.50	0	0
DEAD BOLTS	1.00	3.00	4.00	4	16.00	4	16.00
LOCK SETS	15.00	5.00	20.00	4	80.00	3	60.00
					151.05		109.25
OPENINGS - VENTS, DUCTS, ETC.				BARRIERS			
36" x 36"	10.56	24.10	34.66 (17.33 PER)	2	34.66	2	34.66 34.66
24" x 24"	5.02	22.00	27.02 (13.51 PER)	2	27.02		
					61.68		
ALARM COSTS:							
DETEX PANIC LOCK	68.00	20.00	88.00 EA.	1	88.00	1	88.00
CYPHER LOCKS			193.00 EA	1	193.00	1	193.00
CENTRAL ALARM (BALANCED LINE)			2.0¢/LIN.FT.	250'	500.00	125'	250.00
MODULAR SWITCHES			6.35 EA.	6 EA.	38.10	5	31.75
					819.10		562.75
24 HOUR GUARD POST	22,000./YR		$40,000/YR				
OVERHEAD & MISC.	18,000./YR				$7,519.75		$4,481.14

Figure 2

ing of the windows, securing the doors, establishing the alarms, and securing the air ducts for a total of approximately $7,500. I will not analyze these costs or rationalize why I use a certain type of construction. We have now established rough costs for a SECRET closed production line with the external view of the hardware classified.

The classification of the items produced may have a significant effect on costs insofar as security clearances are concerned. If the hardware to be produced is CONFIDENTIAL, approximately three man hours in production time are utilized for the completion of DD Forms 48-2, DSA Form 482, badging, and briefing. Assuming a starting salary of $2.10 an hour, the CONFIDENTIAL clearance will cost approximately $6.30 in production time per worker for security activities. If a SECRET or TOP SECRET clearance is required, costs increase significantly.

Assume the area we are discussing requires a SECRET clearance. New production workers cannot be given access to the area until they have received a minimum of an interim SECRET clearance. Figure 3 shows the amount of time required by DISCO to process clearances of various degrees. To these times I have added time necessary for processing, briefing, typing, and badging the employees. I have also added ACO approval time for INTERIM clearance and approximate mailing time. These figures indicate the various costs in nonproductive time that it takes to process security clearances. An INTERIM SECRET clearance will cost approximately $235.76. Final SECRET clearances, INTERIM TOP SECRET, and TOP SECRET cost proportionately more. The argument against these costs is that the workers can be placed in training classes or non-classified areas while they are awaiting this clearance. This may be true, but it is far better to reduce the security clearance requirements where possible rather than to make jobs or to reorganize for special situations.

Closed production areas will frequently disrupt the flow of material and personnel. Multiple supply lines must be established. Traffic patterns and work routines are changed for janitors, maintenance personnel, inspectors, engineers, and so forth. These are inconveniences which result in costs which are not easily identified or figured. It may also be necessary to duplicate equipment; one for the closed production line and for the open production line. High capacity equipment such as computerized drills, wave soldering machines, high temperature heat treatment gear, and so forth, are examples of expensive equipment which must be duplicated and will then be run at much less full capacity.

Another type of cost occurring in the operation of closed production lines is that which arises from the need for security and accountability controls. The maintenance of area lists, the control, marking, and accountability for classified hardware, security inspections, changes in stock numbering procedures all create additional expenses.

The contractor can, of course, in one way or the other charge these costs to the User Agencies. CPFF contracts require PCO approval for the expenditure of funds for security purposes. Fixed price contracts include security costs in the initial contract prices. In all other cases, the security costs are buried in overhead or other administrative charges. Despite the potential write-off of these costs, the contractor who does not use every means at his disposal to reduce closed production line costs hurts his business. He submits higher bids and loses contracts. He fails to reduce his expenses, and he reduces his profit. His excessive overhead rates may have an effect on his ability to be a potential bidder.

The question is how to reduce the security costs of the closed area production line and still maintain effective security. To answer this question, I have analyzed a Contract Security Classification Specification,

SECURITY CLEARANCE COSTS

1. DISCO CLEARANCE TIME:

INTERIM SECRET	7 DAYS
SECRET	35 DAYS
INTERIM TOP SECRET (1 DAY IF NAC COMPLETE)	35 DAYS
TOP SECRET	60–100 DAYS
TRANSFERS	1 DAY
MILITARY CONVERSIONS	14 DAYS

2. AVERAGE STARTING PAY FOR PRODUCTION WORKERS: $2.10/HR – $16.80/DAY

3. COMPANY CONFIDENTIAL CLEARANCES:

PROCESSING, BRIEFING, BADGING — 3 HRS ($2.10 × 3 = $6.30 NON-PRODUCTION TIME)

4. INTERIM SECRET CLEARANCES:

PROCESSING, BRIEFING, TYPING, BADGING	1 DAY
ACO APPROVAL TIME	1 DAY
MAIL TIME	5 DAYS
DISCO TIME	7 DAYS
	14 DAYS

14 DAYS AT $16.80/DAY = $235.76 NON-PRODUCTIVE TIME

5. FINAL SECRET CLEARANCES:

SEE ABOVE	14 DAYS
ADDITIONAL DISCO TIME	28 DAYS
	42 DAYS

42 DAYS AT $16.80/DAY = $705.60 NON-PRODUCTIVE TIME

6. INTERIM TOP SECRET:

SEE ABOVE	42 DAYS
ADD 4 DAYS PCO APPROVAL	4 DAYS
	46 DAYS

46 DAYS AT $16.80/DAY = $772.80 NON-PRODUCTIVE TIME

Figure 3

DD Form 254, as it was initially issued to the contractor. Names and places have been changed to protect the guilty. With this 254 we will discuss the original closed area requirements and potential costs. Then, we will examine revised 254s where more specific guidance is given and then determine where the costs have been reduced.

The contract we will discuss is for the production of two types of communications buoys. The original check list, DD Form 254, is shown on Figure 4. This 254 contains several items of interest.

a. Item 10 indicates Access to Communications Analysis Information.

b. The remarks Section of Section 10 indicates special security requirements. In addition, the security cognizance for this contract was awarded to an agency other than DCASR.

c. Item 16 indicates the end item to be SECRET. External view — CONFIDENTIAL. It should be noted that there are two different end items for this contract.

d. The essential elements of information in Item 15 such as frequency, design features, and depth are significant factors in our cost discussions.

I have modified or amended certain features of the DD Form 254 for purposes of this discussion. However, this contract very clearly indicates the effect of classification management on closed area production costs.

This contract resulted in the establishment of a closed area similar to the one shown on Figure 1. It resulted in the division of a major production area. Work was initiated prior to contract award and the DD Form 254 was received approximately 60 days after contract award.

Shortly after contract award and the receipt of the original 254, the project manager, a security administrator, and a classification management specialist examined both the items to be produced under the contract and related them to the security guidance which was furnished. As a result of this study, the following conclusions were reached:

a. One type of buoy was special. It did require access to special information, and it did require security controls. However, this buoy has many parts which were common to the other type of buoy being produced. This buoy became sensitive only during the final production stages. Special access information was used only for research and development studies and was not used in the production phases of the buoys.

b. Based on analysis of component parts, only one type of buoy became a SECRET end item, and then only under special circumstances. With this exception, buoys were CONFIDENTIAL.

c. A further component breakdown study indicated that with minor exceptions all components of both buoys were unclassified and did not become CONFIDENTIAL until major components were assembled.

d. External views of all components were unclassified, and external views of the end items were classified only if certain conditions existed.

e. Elements of information in the DD Form 254-C were in many cases overclassified or were not applicable.

The corporate classification management specialist then prepared a recommended DD 254 for the contract, including a component breakdown chart showing the level of classification of each component and the point in production where some of these items became classified. The proposed DD Form 254 was submitted to the PCO for

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION
(Complete classified items by separate correspondence)

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO PERFORMANCE OF THIS CONTRACT.
FACILITY SECURITY CLEARANCE REQUIRED FOR CONTRACT PERFORMANCE OR FOR ACCESS TO CLASSIFIED INFORMATION IS TOP SECRET

2. THIS SPECIFICATION IS FOR:		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER *(Prime contracts must be shown for all subcontracts)*	DATE TO BE COMPLETED *(Estimated)*	4. THIS SPECIFICATION IS: *(See note below)*		DATED
X	a. PRIME CONTRACT	a. PRIME [illegible]		X	a. ORIGINAL	2/10/71
	b. SUBCONTRACT *(Use Item 8 to identify further subcontracting)*	b. FIRST TIER SUBCONTRACT			b. REVISED *(Supersedes all previous specifications)*	
	c. INVITATION TO BID OR REQUEST FOR PROPOSAL	c. INVITATION FOR BID, REQUEST FOR PROPOSAL, OR REQUEST FOR QUOTE			c. FINAL	

5. IF THIS IS A FOLLOW-ON CONTRACT, ENTER PRECEDING CONTRACT NUMBER AND DATE COMPLETED [X] DOES NOT APPLY

CONTRACT NUMBER

DATE COMPLETED

6a. NAME AND ADDRESS OF PRIME CONTRACTOR *(Include ZIP Code)*

[illegible]

b. NAME AND ADDRESS OF COGNIZANT SECURITY OFFICE *(Include ZIP Code)*

[illegible]

7a. NAME AND ADDRESS OF FIRST TIER SUBCONTRACTOR *(If applicable)* *(Include ZIP Code)*

(Use Item 8 to identify further subcontracting)

b. NAME AND ADDRESS OF COGNIZANT SECURITY OFFICE *(Include ZIP Code)*

8. SUBCONTRACTING BEYOND FIRST TIER *(as appropriate)*

9a. GENERAL IDENTIFICATION OF THE PROCUREMENT FOR WHICH THIS SPECIFICATION APPLIES

COMMUNICATION BUOYS

b. CONTRACT PRESCRIBES SECURITY REQUIREMENTS WHICH ARE ADDITIONAL TO THOSE PRESCRIBED IN DD FORM 441 AND THE ISM [X] YES [ ] NO

10. CONTRACT PERFORMANCE WILL REQUIRE	YES	NO
GRAPHIC ARTS SERVICES		X
ACCESS TO CONTROLLED AREAS OF CLASSIFIED INFORMATION ONLY	X*	
MANUFACTURE OF CLASSIFIED HARDWARE	X	
GENERATION, RECEIPT, OR CUSTODY OF CLASSIFIED DOCUMENTS OR OTHER MATERIAL	X	
ACCESS TO RESTRICTED DATA		X
ACCESS TO CRYPTOGRAPHIC INFORMATION		X
ACCESS TO COMMUNICATION ANALYSIS INFORMATION	** X	
DEFENSE DOCUMENTATION CENTER OR DEFENSE INFORMATION ANALYSIS CENTER SERVICES WILL BE REQUESTED [illegible]		X

REMARKS

*This contract requires access to communications analysis information. The [illegible] has exclusive security responsibilities for this contract. See Item 13.

**TOP SECRET clearance is required for access to [illegible]

11. REFER ALL QUESTIONS PERTAINING TO CONTRACT SECURITY CLASSIFICATION SPECIFICATION TO THE OFFICIAL NAMED BELOW *(NORMALLY, thru ACO (Item 6b), EMERGENCY [illegible] with written record of inquiry and response to ACO) (thru prime contractor for subcontracts)*

a. PROGRAM/PROJECT MANAGER ACTIVITY *(Name, Title, and Organization)*

[illegible]

b. ADDRESS, TELEPHONE NUMBER AND OFFICE SYMBOL *(Include ZIP Code)*

[illegible]

NOTE: Original Specification (Item 4a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 4b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual

DD FORM 254 REPLACES EDITION OF 1 DEC 65 AND DD FORM 254-1, WHICH ARE OBSOLETE. PAGE 1 OF 4 PAGES

Figure 4
Part 1

information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual *(paragraph 5n and Appendix IX)*.

PROPOSED PUBLIC RELEASES SHALL BE SUBMITTED FOR APPROVAL PRIOR TO RELEASE ☐ DIRECT ☐ THROUGH *(Specify)*

illegible

TO THE DIRECTORATE FOR SECURITY REVIEW, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE *(Public Affairs)** FOR REVIEW IN ACCORDANCE WITH PARAGRAPH 5n OF THE INDUSTRIAL SECURITY MANUAL.

** In the case of non-DoD User agencies, see footnote, paragraph 5n, Industrial Security Manual.*

SECURITY CLASSIFICATION SPECIFICATIONS FOR THIS CONTRACT ARE SET FORTH BELOW *(Check which are applicable)*:

☒ DD FORM 254C ATTACHED *(hereby made a part of this specification)*.

☐ DOCUMENT(S) LISTED BELOW *(hereby made part of this specification)*.

☒ AS STATED BELOW

A. This contract requires access to sensitive intelligence information. Contractor personnel will be briefed and will sign appropriate security briefing statements as directed by illegible. Contractor will maintain records of all individuals given access to information pertaining to this contract.

CONTRACT SECURITY CLASSIFICATION SPECIFICATIONS FOR SUBCONTRACTS ISSUING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIAL NAMED IN ITEM 14b BELOW.

REQUIRED DISTRIBUTION:

☒ PRIME CONTRACTOR *(Item 6a)*

☒ COGNIZANT SECURITY OFFICE *(Item 6b)*

☒ ADMINISTRATIVE CONTRACTING OFFICE *(Item 14b)*

☐ MATERIAL INSPECTOR

☐ DIRECTOR, FEDERAL BUREAU OF INVESTIGATION WASHINGTON, D.C *(Only for Items 2a and 2b) (Attachments hereto not included.)*

☐ SUBCONTRACTOR *(Item 7a)*

☐ COGNIZANT SECURITY OFFICE *(Item 7b)*

ADDITIONAL DISTRIBUTION:

☒ illegible

☒ illegible

14. THIS CONTRACT SECURITY CLASSIFICATION SPECIFICATION AND ATTACHMENTS REFERENCED HEREIN, APPROVED BY THE USER AGENCY CONTRACTING OFFICER OR HIS REPRESENTATIVE NAMED BELOW:

SIGNATURE

TYPED NAME AND TITLE OF APPROVING OFFICIAL

JOHN BROWN

c. APPROVING OFFICIAL'S ACTIVITY AND ADDRESS *(Include ZIP Code)*

illegible

b. NAME AND ADDRESS OF ADMINISTRATIVE CONTRACTING OFFICE *(Include Zip Code)*

illegible

PAGE 2 OF 4 PAGES

Figure 4
Part 2

DEPARTMENT OF DEFENSE

CONTRACT SECURITY CLASSIFICATION SPECIFICATION *(Continued)*

PART OF DD FORM 254, DATED 2/10/71 (from item 4) FOR CONTRACT NO. (from item 3)

15. For definitions of items appearing in the following pre-printed list, see Industrial Security Regulation, Section IX, or Industrial Security Manual, Appendix I, paragraph 1. In the "Remarks" column or in appended attachments reference in the "Remarks" column, elaborate and explain sufficiently to identify clearly and precisely the information which requires classification. Provide downgrading and declassification instructions either by stating specific dates, times, or events or by group marking for each item classified.

ELEMENTS OF INFORMATION	CLASSIFICATION	GROUP	REMARKS
a. ACCURACY:			
(1)	S	3	
(2)			
b. ALTITUDE:			
(1)	N/A		
(2)			
c. COUNTER COUNTERMEASURES CAPABILITY:			
(1)			
(2)			
d. DEPTH:			
(1)	S	3	
(2)			
e. DESIGN INFORMATION:			
(1)	S	3	
(2)			
f. FORMULA OR MATERIAL:			
(1)	U	-	
(2)			
g. FUEL/PROPELLANT:			
(1) TYPE	N/A		
(2) CONSUMPTION			
(3) CAPACITY			
h. LETHALITY/CRITICAL EFFECTS:			
(1)	N/A		
(2)			
i. MANEUVERABILITY:			
(1)	S	3	
(2)			
j. OPERATIONAL READINESS (Alert) TIME/TIME CYCLE:			
(1)	S	3	
(2)			
k. ORBIT/TRAJECTORY:			
(1)	N/A		
(2)			
l. RANGE:			
(1)	C	3	
(2)			

DD FORM 1 JUL 67 254c

PAGE 3 OF 4 PAGES

Figure 4
Part 3

15. (Continued) ELEMENTS OF INFORMATION	CLASSIFICATION	GROUP	REMARKS
m. RELIABILITY:			
(1)	U	-	
(2)			
n. RESOLUTION:			
(1)	N/A		
(2)			
o. SIGNATURE CHARACTERISTICS:			
(1)	S	3	
(2)			
p. SPEED/VELOCITY:			
(1) MAXIMUM	N/A		
(2) CRUISING			
(3) TAKE-OFF OR LAUNCHING			
(4) LANDING			
(5) ACCELERATION AND/OR DECELERATION			
q. SYSTEM CAPACITY:			
(1)	C	3	
(2)			
r. TERMINAL BALLISTICS:			
(1)	N/A		
(2)			
s. THRUST:			
(1) CLASS	N/A		
(2) SPECIFIC			
(3) SPECIFIC IMPULSE			
t. VULNERABILITY:			
(1)	N/A		
(2)			
(Add additional items)			
u.			
16. END ITEM PRODUCED			
a. CLASSIFICATION OF END ITEM	S	3	
b. VIEW	C	3	
c. MILITARY APPLICATION	S NOFORN	3	
d. NUMBERS CONTRACTED	U		
e. PRODUCTION AND PROGRAM SCHEDULES	U		
f. RATE OF DELIVERY	U		
g. NUMBERS DELIVERED	U		
h. DEGREE OF PROTECTION IN TRANSIT			
i. UNIT COST	U		
j. OTHER: (Add additional sheets if necessary.)			
k.			

PAGE 4 OF 4 PAGES

Figure 4
Part 4

approval. It was accepted and the new DD Form 254 is shown on Figure 5.

What were the results of this classification management review?

a. The size of the closed production area was reduced from 150 feet x 75 feet to 75 feet x 39 feet. This is shown on Figure 6. Referring you again to the costs on Figure 2, you will notice that the costs are reduced from approximately $7,500 to approximately $4,480, a savings of some $3,000 odd dollars.

b. SECRET clearance and special briefing are now required for only 30 production workers out of approximately 150. In addition no nonproductive time was wasted in obtaining INTERIM SECRET clearances. The net savings was approximately 14 man days per employee of production time.

c. There was no disruption or reorganization of a major production area.

d. Special briefings were not required except for engineers and technical personnel, and sensitive information was more fully protected.

e. Proposals for follow-on contracts based on new classification philosophies resulted in savings to both the government and the contractor and additional contracts for the contractor.

This case was one of several where we were able to show a reduction in the cost of closed production lines through classification management studies. It should also be obvious that there are many other security savings resulting from these studies. To effectively reduce costs in a closed production area, the classification management studies should include the following:

a. A detailed study of component breakdowns and classifications.

b. Specific determination of what information is classified and at what point in the production line the classified information is disclosed.

c. An analysis of assembly procedures to reduce closed area size and cost.

d. An analysis of the need for special controls, special access, visual and aural access, and similar requirements which relate more to the protection of information rather than to the protection of things.

Classification management analysis and studies should be initiated during research and development and study contracts. Closed and restricted areas utilized for the production of breadboards, preproduction models, STMs and so forth, do not fall into the category of closed production lines. However, security problems in that area can be studied and used in the establishment of closed production lines. Many times the prime contracting officer awards a production contract and issues the same security guidance that was used for research and development study contracts. This is obviously a fallacy. State-of-the-art changes, general release of information, and the tactical use of equipment result in the downgrading of most production models. Negotiations for production contracts for classified hardware and equipment should include a review of security requirements. Government and contractor, engineering, classification management, and contract administration personnel should analyze the security requirements prior to contract award. Security cost studies should be included. Government should seek the advice of production contractors as they are often more familiar with the details of the hardware to be produced. Contractors should be requested to establish security guidance for end items and individual components. Many

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION
(Complete classified items by separate correspondence)

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO PERFORMANCE OF THIS CONTRACT.
FACILITY SECURITY CLEARANCE REQUIRED FOR CONTRACT PERFORMANCE OR FOR ACCESS TO CLASSIFIED INFORMATION IS CONFIDENTIAL

2. THIS SPECIFICATION IS FOR:		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER *(Prime contracts must be shown for all subcontracts)*	DATE TO BE COMPLETED *(Estimated)*	4. THIS SPECIFICATION IS: *(See note below)*		DATED
X	a. PRIME CONTRACT	a. PRIME ulchy oho llol yllo lucynollo			a. ORIGINAL	
	b. SUBCONTRACT *(Use Item 8 to identify further subcontracting)*	b. FIRST TIER SUBCONTRACT		X	b. REVISED *(Supersedes all previous specifications)*	6/10/71
	c. INVITATION TO BID OR REQUEST FOR PROPOSAL	c. INVITATION FOR BID, REQUEST FOR PROPOSAL, OR REQUEST FOR QUOTE			c. FINAL	

5. IF THIS IS A FOLLOW-ON CONTRACT, ENTER PRECEDING CONTRACT NUMBER AND DATE COMPLETED [X] DOES NOT APPLY

CONTRACT NUMBER	DATE COMPLETED

6a. NAME AND ADDRESS OF PRIME CONTRACTOR *(Include ZIP Code)*	b. NAME AND ADDRESS OF COGNIZANT SECURITY OFFICE *(Include ZIP Code)*
oulh ulnouyc ou loulo ull. lyu ou luucu yuu luoju lluuc ouy ulchy oho llol yllo ilo du	ulchy oho llol yllo lucynollo du cyulluo :lhoul luc ylu uu · cluo , llo. oulh ulnouyc ou loulo cllo y l

7a. NAME AND ADDRESS OF FIRST TIER SUBCONTRACTOR *(If applicable) (Include ZIP Code)* *(Use Item 8 to identify further subcontracting)*	b. NAME AND ADDRESS OF COGNIZANT SECURITY OFFICE *(Include ZIP Code)*

8. SUBCONTRACTING BEYOND FIRST TIER *(as appropriate)*

9a. GENERAL IDENTIFICATION OF THE PROCUREMENT FOR WHICH THIS SPECIFICATION APPLIES

COMMUNICATIONS BUOYS A-SILENT
B-STANDARD

b. CONTRACT PRESCRIBES SECURITY REQUIREMENTS WHICH ARE ADDITIONAL TO THOSE PRESCRIBED IN DD FORM 441 AND THE ISM [ ] YES [X] NO

10. CONTRACT PERFORMANCE WILL REQUIRE	YES	NO
GRAPHIC ARTS SERVICES		X
ACCESS TO CONTROLLED AREAS OR CLASSIFIED INFORMATION ONLY	X*	
MANUFACTURE OF CLASSIFIED HARDWARE	X	
GENERATION, RECEIPT, OR CUSTODY OF CLASSIFIED DOCUMENTS OR OTHER MATERIAL	X	
ACCESS TO RESTRICTED DATA		X
ACCESS TO CRYPTOGRAPHIC INFORMATION		X
ACCESS TO COMMUNICATION ANALYSIS INFORMATION	NOTE 1	
DEFENSE DOCUMENTATION CENTER OR DEFENSE INFORMATION ANALYSIS CENTER SERVICES MAY BE REQUESTED *(If yes see paragraph 7, app I, Industrial Security Manual)*		X

REMARKS

NOTE 1 The portion of this contract pertaining to buoy A requires access to Communications Analysis Information for background and development purposes. The cllo yllouulo oh oulh ulnouyc · cllo /llouulo oh oulh ulnouyc ou loulo ull. clo olo yllqu has exclusive security responsibility for this portion of the contract. See Item 13.

*TOP SECRET clearance is required for access to lyu ou luucu yuu luoju lluuc ouy olo cyulluo oluuulchy.

11. REFER ALL QUESTIONS PERTAINING TO CONTRACT SECURITY CLASSIFICATION SPECIFICATION TO THE OFFICIAL NAMED BELOW *(NORMALLY, thru ACO (Item 14b); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts)*

a. PROGRAM PROJECT MANAGER OR ACTIVITY *(Name, Title, and Organization)*	b. ADDRESS TELEPHONE NUMBER AND OFFICE SYMBOL *(Include ZIP Code)*
cliouh luc ylu uu ı lyu ou luucu yuu luoju lluuc ouy ulchy oho llol yllo ı nollo u	du cyulluo oluuulchy oho llol ı lucyı clh ylu ou

NOTE: *Original Specification (Item 4a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 4b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.*

DD FORM 1 JUL 67 254 — REPLACES EDITION OF 1 DEC 65 AND DD FORM 254-1, WHICH ARE OBSOLETE. — PAGE 1 OF 4 PAGES

Figure 5
Part 1

... pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be ... public dissemination except as provided by the Industrial Security Manual (*paragraph 5n and Appendix IX*).

PROPOSED PUBLIC RELEASES SHALL BE SUBMITTED FOR APPROVAL PRIOR TO RELEASE ☐ DIRECT ☐ THROUGH (*Specify*)

clno yollonk lnn clo donclhonh lnc ylnn on t clno yollonk lnn clo donolno llol yllo lncynollo , lncynn.

TO THE DIRECTORATE FOR SECURITY REVIEW, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (*Public Affairs*)* FOR REVIEW IN ACCORDANCE WITH PARAGRAPH 5n OF THE INDUSTRIAL SECURITY MANUAL.

*In the case of non-DoD user agencies, see footnote, paragraph 5n, Industrial Security Manual.

SECURITY CLASSIFICATION SPECIFICATIONS FOR THIS CONTRACT ARE SET FORTH BELOW (*Check which are applicable*):

☒ DD FORM 254C ATTACHED (*hereby made a part of this specification*).

☐ DOCUMENT(S) LISTED BELOW (*hereby made part of this specification*).

☒ AS STATED BELOW

A. Background and development information for buoy A requires access to sensitive intelligence information. Contractor personnel given access to this information will be briefed and will sign appropriate Security Briefing Statements as directed by oulh ulnooyc oun lonlo oll t cllo yllonulo ol oulh ulnooyc oun lonlo oll t cllo yllonulo . This information will not be released to production areas.

CONTRACT SECURITY CLASSIFICATION SPECIFICATIONS FOR SUBCONTRACTS ISSUING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIAL NAMED IN ITEM 14b BELOW.

REQUIRED DISTRIBUTION:	14. THIS CONTRACT SECURITY CLASSIFICATION SPECIFICATION AND ATTACHMENTS REFERENCED HEREIN, APPROVED BY THE USER AGENCY CONTRACTING OFFICER OR HIS REPRESENTATIVE NAMED BELOW
☒ PRIME CONTRACTOR (*Item 6a*) ☒ COGNIZANT SECURITY OFFICE (*Item 6b*) ☒ ADMINISTRATIVE CONTRACTING OFFICE (*Item 14b*) ☐ MATERIAL INSPECTOR	SIGNATURE
☐ DIRECTOR, FEDERAL BUREAU OF INVESTIGATION WASHINGTON, D.C. (*Only for Items 2a and 2b*) (*Attachments hereto not included.*)	TYPED NAME AND TITLE OF APPROVING OFFICIAL JOHN BROWN
☐ SUBCONTRACTOR (*Item 7a*) ☐ COGNIZANT SECURITY OFFICE (*Item 7b*) ADDITIONAL DISTRIBUTION:	a. APPROVING OFFICIAL'S ACTIVITY AND ADDRESS (*Include ZIP Code*) olo yllqoo lyu on lnncn cyullno olnulchy olno llol , lo nollo ıl
☒ ☒	b. NAME AND ADDRESS OF ADMINISTRATIVE CONTRACTING OFFICE (*Include Zip Code*) lnn clo don 'lonulo you lnoyo llnoc ony olo , llyon lyu on

PAGE 2 OF 4 PAGES

Figure 5
Part 2

DEPARTMENT OF DEFENSE

CONTRACT SECURITY CLASSIFICATION SPECIFICATION *(Continued)*

PART OF DD FORM 254, DATED 6/10/71 *(from item 4)* FOR CONTRACT NO. _____ *(from item 3)*

15. For definitions of items appearing in the following pre-printed list, see Industrial Security Regulation, Section IX, or Industrial Security Manual, Appendix I, paragraph 1. In the "Remarks" column or in appended attachments reference in the "Remarks" column, elaborate and explain sufficiently to identify clearly and precisely the information which requires classification. Provide downgrading and declassification instructions either by stating specific dates, times, or events or by group marking for each item classified.

ELEMENTS OF INFORMATION	CLASSIFICATION	GROUP	REMARKS
a. ACCURACY: (1)	N/A		
(2)			
b. ALTITUDE: (1)	N/A		
(2)			
c. COUNTER COUNTERMEASURES CAPABILITY: (1)	N/A		
(2)			
d. DEPTH: (1)	NOTE 1 C	III	NOTE 1 - Depth at which buoys are launched.
(2)			
e. DESIGN INFORMATION: (1)	N/A		
(2)			
f. FORMULA OR MATERIAL: (1)	N/A		
(2)			
g. FUEL/PROPELLANT: (1) TYPE	N/A		
(2) CONSUMPTION			
(3) CAPACITY			
h. LETHALITY/CRITICAL EFFECTS: (1)	N/A		
(2)			
i. MANEUVERABILITY: (1)	N/A		
(2)			
j. OPERATIONAL READINESS *(Alert)* TIME/ TIME CYCLE: (1)	N/A		
(2)			
k. ORBIT/TRAJECTORY: (1)	N/A		
(2)			
l. RANGE: (1)	N/A		
(2)			

DD FORM 1 JUL 67 254c

PAGE 3 OF 4 PAGES

Figure 5
Part 3

15. (Continued) ELEMENTS OF INFORMATION	CLASSIFICATION	GROUP
m. RELIABILITY: (1)	N/A	
(2)		
n. RESOLUTION: (1)	N/A	
(2)		
o. SIGNATURE CHARACTERISTICS: (1)	NOTE 2 C	III
(2)		
p. SPEED/VELOCITY: (1) MAXIMUM	NOTE 3 C	III
(2) CRUISING		
(3) TAKE-OFF OR LAUNCHING		
(4) LANDING		
(5) ACCELERATION AND/OR DECELERATION		
q. SYSTEM CAPACITY: (1)	NOTE 4 C	III
(2)		
r. TERMINAL BALLISTICS: (1)	N/A	
(2)		
s. THRUST: (1) CLASS	N/A	
(2) SPECIFIC		
(3) SPECIFIC IMPULSE		
t. VULNERABILITY: (1)	N/A	
(2)		
u. OTHER: (Specify. Add additional sheets if necessary.)		
v.		
16. END ITEM PRODUCED	NOTE 6	
a. CLASSIFICATION OF END ITEM	C	III
b. EXTERNAL VIEW	U	NOTE 6
c. MILITARY APPLICATION	C	III
d. NUMBERS CONTRACTED	U	
e. PRODUCTION AND PROGRAM SCHEDULES	SEE REMARKS	
f. RATE OF DELIVERY	U	
g. NUMBERS DELIVERED	U	
h. DEGREE OF PROTECTION IN TRANSIT	C	III
i. UNIT COST	U	
j. OTHER: (Add additional sheets if necessary.)		
k.		

REMARKS

NOTE 2 - Specific preset buoy frequency-when related to buoy serial number or groups of buoy serial numbers.

NOTE 3 - Maximum launch speed required and/or attainable.

NOTE 4 - Length of message, transmission cycle, transmission duration, buoy transmission life.

NOTE 5 - a. Specific operational destinations
b. Specific operational vehicles
c. Specific operational use

NOTE 6 - See attached component breakdown.

NOTE 5

--Association of production schedules with destination points is classified CONFIDENTIAL, Group 3.

PAGE 4 OF 4 PAGES

Figure 5
Part 4

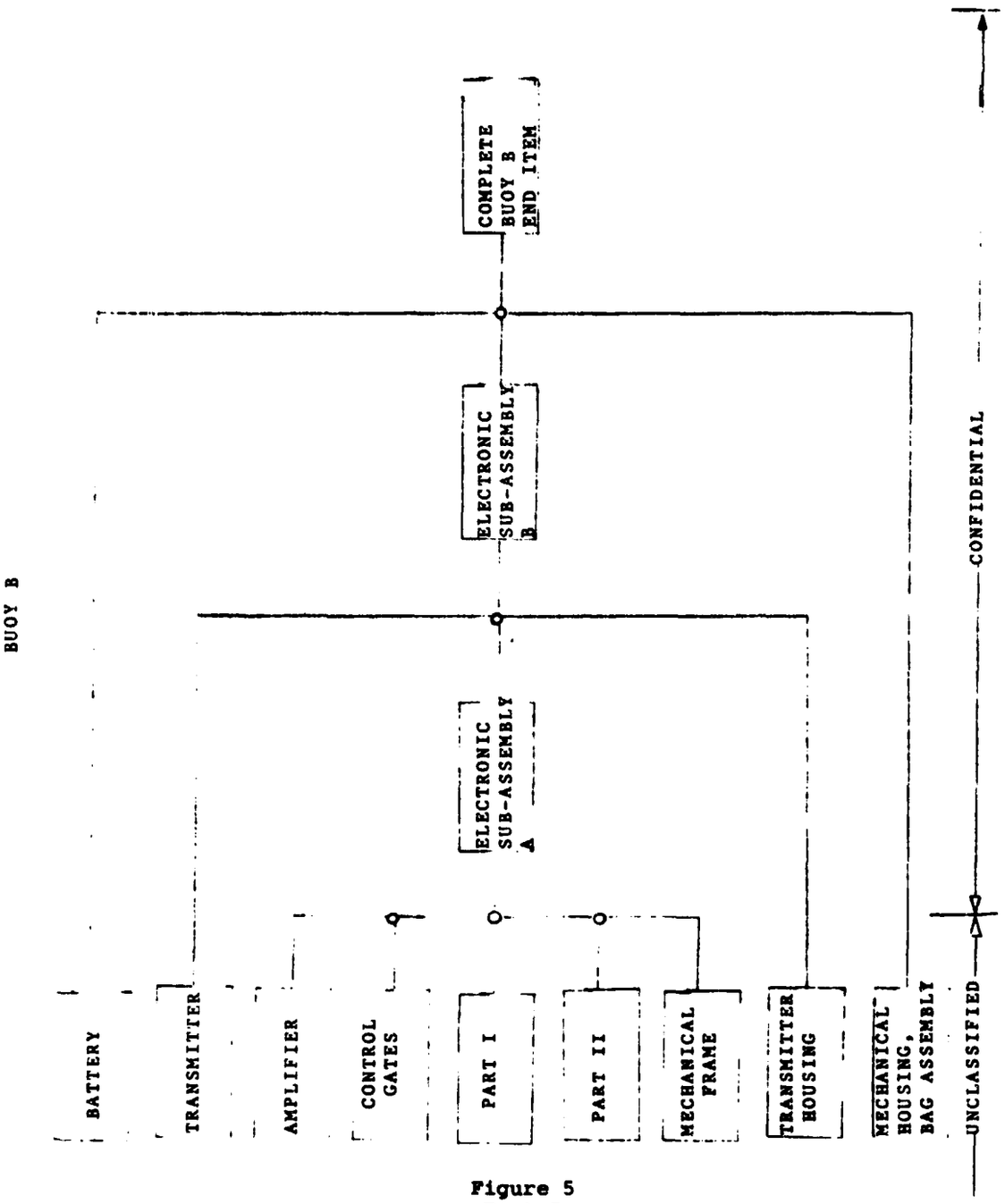


Figure 5
Part 5

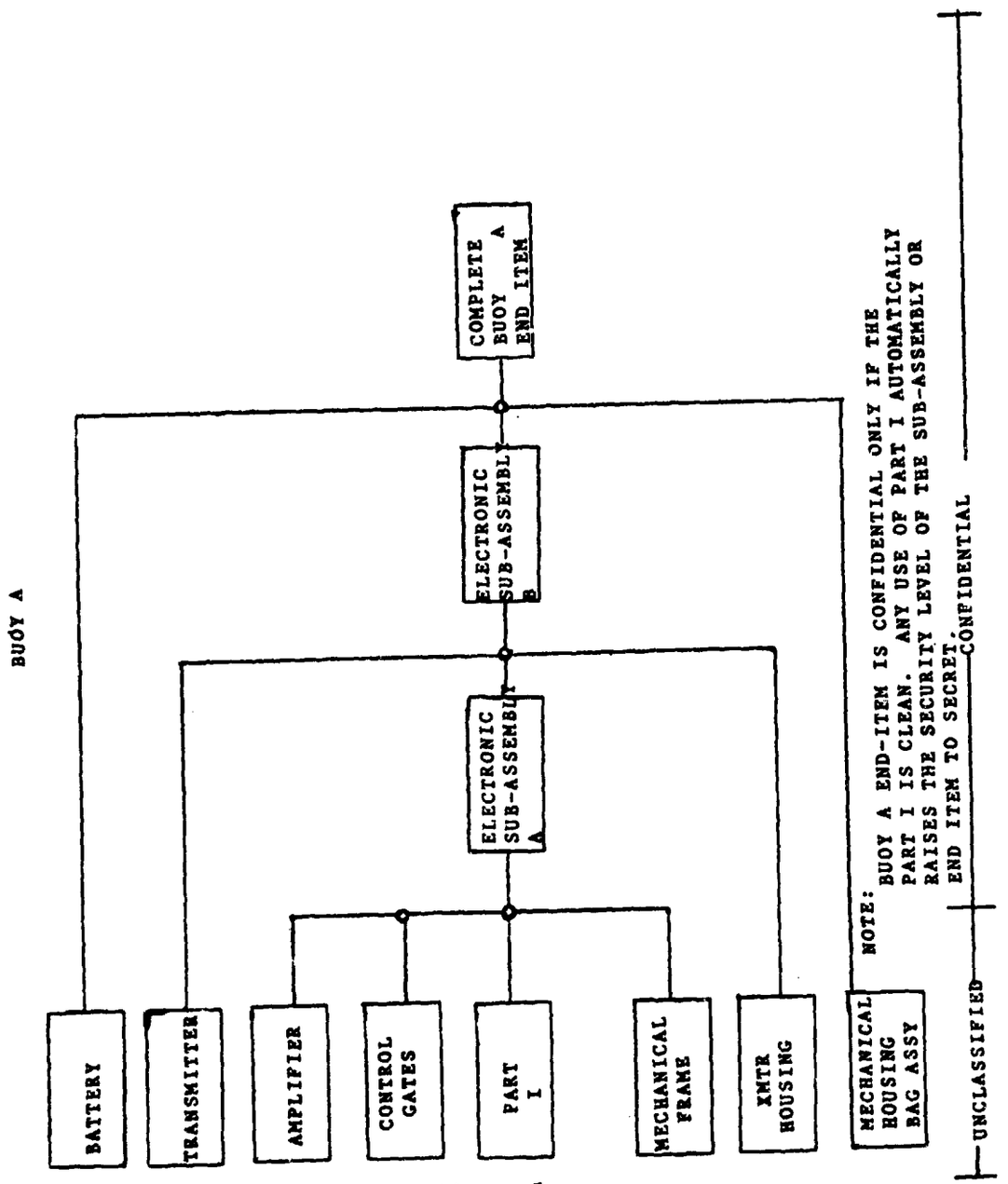


Figure 5
Part 6

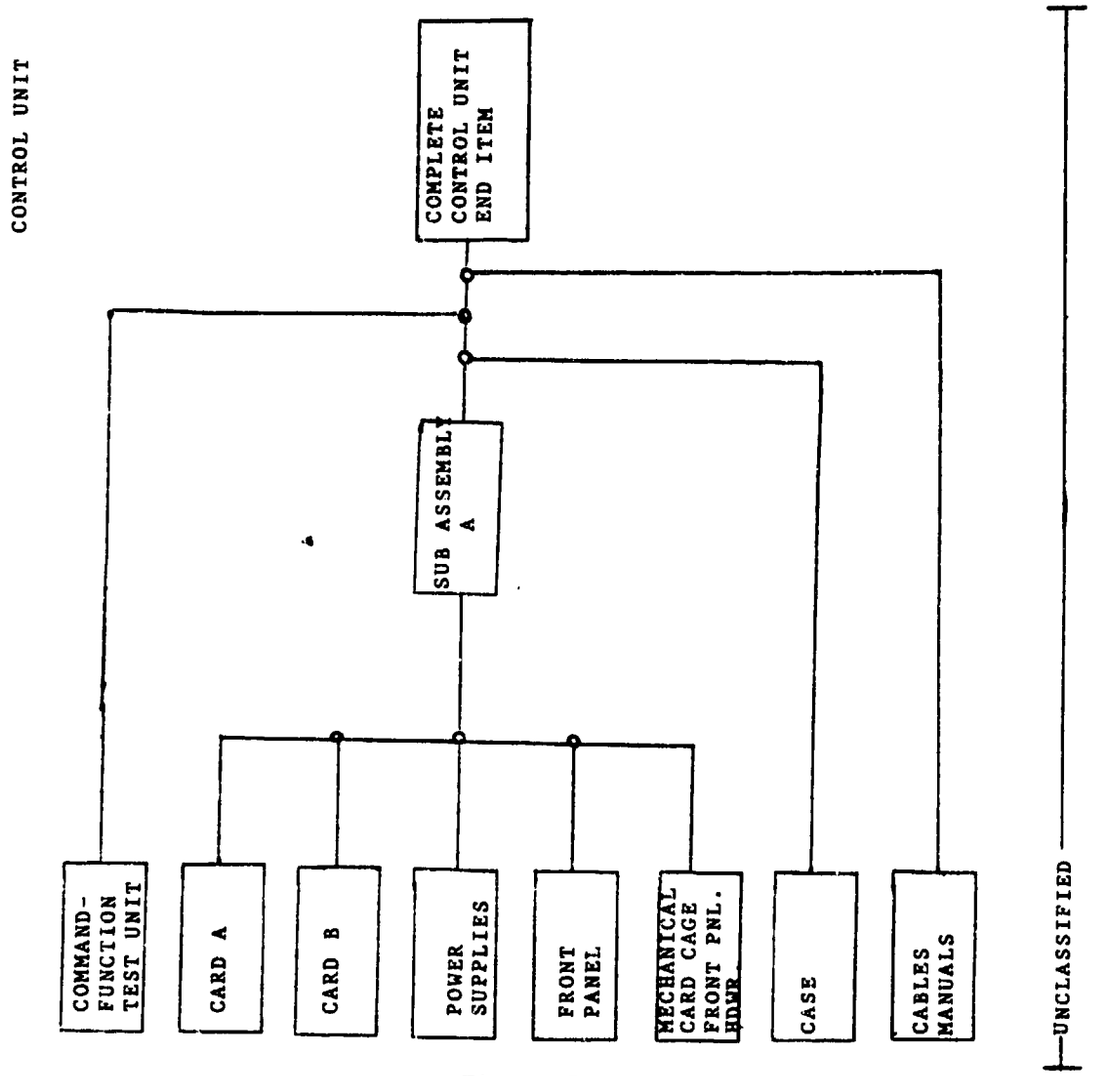


Figure 5.
Part 7

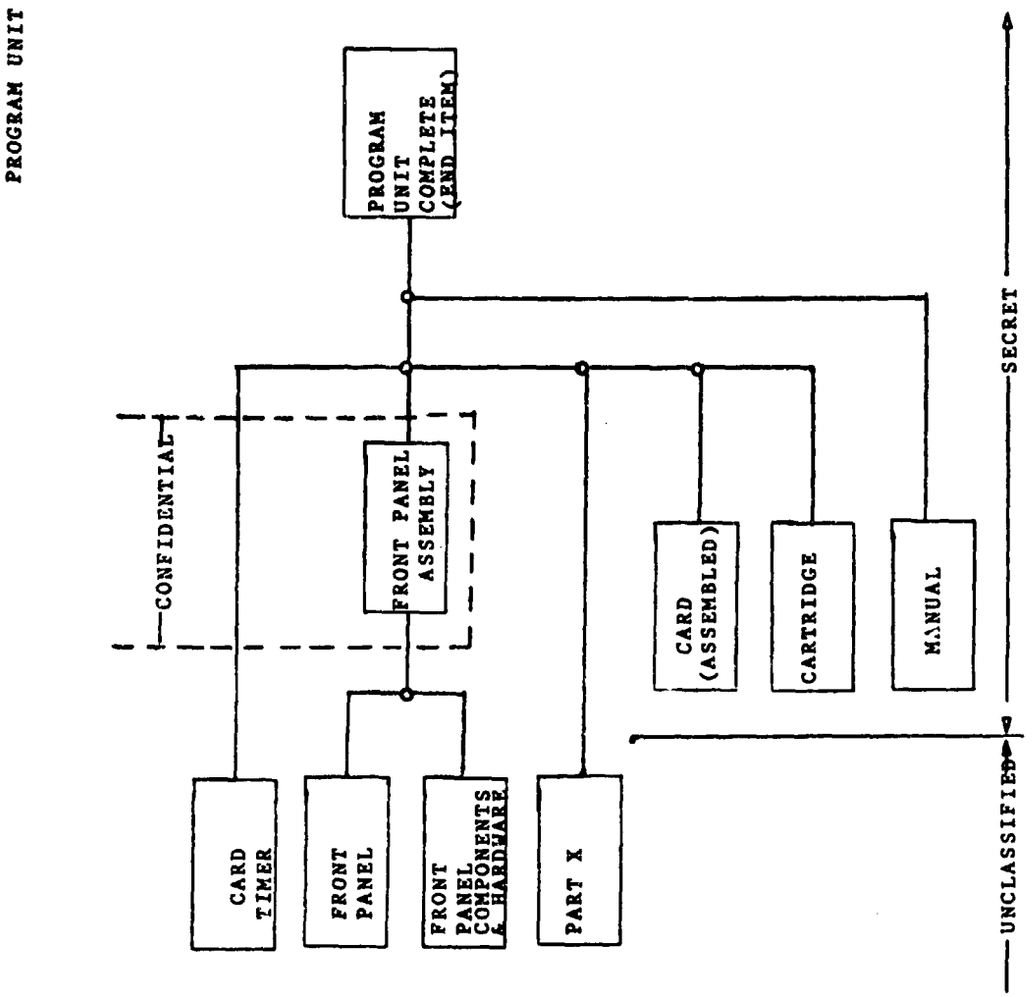
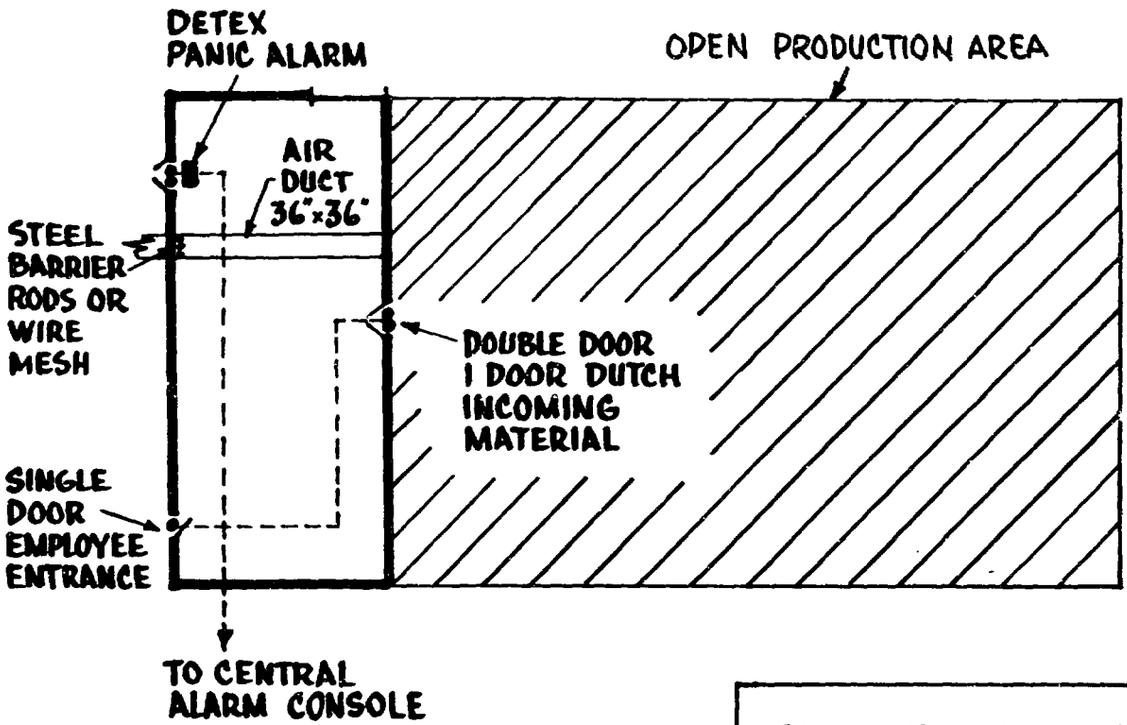


Figure 5
Part 8

FINAL CLOSED PRODUCTION AREA



CEILING HEIGHT-----14'
AREA -------75'L x 30'W
WINDOWS -----12'W x 8'H

Figure 6

contractors take this action voluntarily in order to save money. If this is done, government must establish procedures for the rapid review and revision of security guidance.

We are all well aware that the Department of Defense paperwork machinery is fantastic in its size and in its slowness; but when contractors submit adequate and appropriate security guidance for review and possible dissemination, it should not take 60, 90, or 180 days to have it accepted and published. Complete and adequate security guidance should be available to the contractor prior to contract award. Then, whenever the contractor submits a recommendation for a change or improvement in the security guidance which would result in savings to both the contractor and the government, there should be a special channel for immediate positive action for the acceptance and issuance of the new DD Form 254 or for immediate disapproval.

Remarks of Arthur F. Van Cook —

One of the stated objectives of the Defense Classification Management Program is to "eliminate unnecessary expense to the Department of Defense and Industry incurred in protecting information which no longer requires security protection." This particular objective will be fully achieved only when overclassification is eliminated. By overclassification, I mean either affording information or material a higher degree of security classification protection than is necessary at the outset or not downgrading or declassifying information or material already classified when it is found that it warrants a lower degree or no longer warrants any degree of such protection in the interests of national defense. In short, when we get to the point where security classification protection is afforded to only that information or material which truly requires protection in the national defense interests, any expense associated with the safeguarding of that information or material will be a necessary and justifiable one. We, of course, have not reached that point but we continually strive to get there. We must also strive to bring about a reduction in spiraling security costs including those believed to be necessary and even justifiable. I believe this latter goal to be realistic and more near term than the former.

At the outset, let's dispel any illusion that some in this audience may have that we are here today to attempt to hang a price tag on our nation's secrets. I don't profess to know how to go about that and I will challenge the man who does. For example, this kind of question, in my opinion, defies a reasonable response: What is the dollar value one places on a secret, the unauthorized disclosure of which would permit an enemy or potential enemy to develop countermeasures which would nullify the effectiveness of a defensive weapons system costing several billions — a system designed to save an unknown number of human lives?

Our interest here today is to discuss ways and means of identifying security costs associated with the safeguarding of our secrets and to focus attention on those areas where it is believed that such costs may be reduced or avoided through good classification management practices without loss of security.

It is a known fact that the security costs with which we are concerned run high. When one considers the costs of such necessary things as document control, guard and alarm systems, security containers and personnel clearances, on a worldwide basis, it can be safely assumed that these costs run into many millions annually.

Experience has shown that security costs which we seek to identify are not easily obtainable and when they are gathered, even on a representative basis, are not easily validated. Part of the reason for this is that in industry, security costs are shrouded in something called "overhead," while

in defense, they are wrapped in a label called "administrative costs." Another, and more important part of the reason, is the unexplained reluctance on the part of some people in our business to dig, find, and report.

Top management in both defense and industry, have, in recent years, opened their eyes to the fact that good classification management practices can save dollars and have given unprecedented support to the program. This was accomplished by reporting to them on a representative basis, examples of specific dollars saved or avoided through correct initial classification, downgrading and declassification. Continuing support from the top management level is needed to better effectuate the classification management program in both defense and industry. Thus, there is a need for factual reports, not only for top management but for public consumption as well, of examples of dollars saved or avoided by classification management — eye opening reports — to be developed and publicized on a continuing basis. First, however, studies are required to be developed which will provide a base for all to use on which can be measured the effectiveness of a particular classification management program designed in part to reduce security costs. There have been several security cost studies developed in the past by activities in both defense and industry, some of which you are familiar with.

One that gained much attention was a study produced by a large industrial firm a few years ago. It concluded that it cost that firm at that time $7.18 to generate and maintain one Secret document on an annual basis versus $2.11 for a Confidential one. I am sure that most of you are familiar with those numbers. The study was an excellent one for its use as a classification management tool for that particular firm. In developing the $7.18 and $2.11 annual per document cost, they considered the total direct and indirect costs involved and correlated them to their then current classified inventory. When these per document costs were publicized, however, they were picked up and wrongly used by many without regard to the user's own direct and indirect costs. For example, one defense activity, in connection with a classified document review program, reported to our office that it cost that activity an estimated $11 million during one particular calendar year to safeguard 3.2 million Confidential and Secret documents. Upon inquiry, I was told that the $11 million estimate was based on the per document cost developed by the industrial firm study multiplied by the number of Secret and Confidential documents in the defense activity's then current inventory. I understand that no consideration was given to the direct and indirect costs which were applicable to that particular defense activity — such costs widely varying from those of the industrial firm which produced the study. In another instance, a defense activity reported a cost avoidance of close to three-quarters of a million dollars in connection with a program designed to reduce the Defense Top Sectet inventory. I questioned this reported cost avoidance and found that it too was based in large part on the study developed by the industrial firm. In this case, the defense activity representative responsible for preparing the report stated that if it cost $7.18 to maintain a Secret document for one year, then $10.00 would be a fair estimate for a Top Secret one. Therefore, if his activity, as it did, reduced its Top Secret inventory by 75,000 documents — a cost avoidance of $750,000 would accrue.

These are examples of people playing, albeit in good faith, the "numbers game." Neither we, as classification managers, nor people at the top management level are interested in playing games of any kind — particularly those involving numbers which cannot be validated. If the cost data we develop are not factual, it is not reportable.

As mentioned earlier, we need to form a base for computation of meaningful security cost data. There are many

factors to be considered in developing such a base and there are as many ways of going about it. I will propose one method today for your consideration.

I have no quarrel with the method of tying direct and indirect security costs to numbers of classified documents held provided the per document cost figure which results is used exclusively by the activity which determined it for whatever purposes they desire. However, I would point out that in using such a method, the per document cost figure fluctuates, though not in direct ratio, but to some degree with a change in the volume of documents held in classified inventories. I say not in direct ratio because some of the costs, especially the indirect ones, remain constant regardless of the numbers of classified documents held.

I would propose that perhaps 20 representative industrial firms performing on classified contracts and as many representative defense activities handling classified material, participate in an effort, on a voluntary basis, to establish a meaningful security cost data base which may be used throughout defense and industry to measure the effectiveness of programs designed to reduce costs which are associated with the safeguarding of classified information or material.

These participating activities would, on an individual basis, determine the average hourly wage rates of personnel engaged in such functions as classified document marking, processing, transmission, inventorying, and retrieval together with the average time spent in performing each of these functions. In determining these averages, each participating activity would use the same sample classified material for study purposes. For example, each would process a sample memorandum with a specific subject and a specific number of pages classified at the Top Secret, Secret and Confidential level. Each such memorandum would be actually marked, processed and transmitted with records kept of the personnel time involved which could be correlated to hourly wage rates. Each of the participating activities would report the results of their respective time-cost study to some central office, preferably ours, where all the data could be compiled, averaged, and disseminated for use throughout defense and industry. The compilation would show, for example, the average base direct cost of marking a classified document of 5 or 50 pages, or the average direct cost of preparing receipts, logs and envelopes for a 5 or 50 page Top Secret, Secret or Confidential document or the average cost of inventorying a Top Secret or Secret document. Cost data could also be gathered from these participating activities on such other things as security containers, guard and alarm systems, security clearances, and maintenance, on a current basis, of accountability records. This proposal would not entail the correlation of direct and indirect costs to classified inventories held by the participating activities as has been done with past studies of this kind.

The method of developing security cost data which I have briefly outlined here would provide classification managers with average base costs which could be applied "across the board" to any results derived from the effective implementation of special programs designed, in part, to reduce security costs. For example, if an industrial or defense facility undertook to clear out its files — an exercise which is, incidentally, currently underway in the Department of Defense — and, as a result of that program, found that a specific number of classified documents, subject to inventory requirements, were eliminated, that facility would have readily available, on a per document basis, an average base cost figure for the conduct of classified document inventory — a valid figure which could be applied to show the cost avoidance accomplished by the particular program.

We have received reports from User Agencies which show that contracts, once classified, have now been de-

classified through the efforts of classification managers in both defense and industry working in concert. In these cases, we are aware that much effort went into bringing about these declassification actions. When we in defense or you in industry are asked what benefits are derived from such action, the response is expected to be expressed in terms of dollars saved. Such response is hard to come by because any estimate to what these savings might be would be wholly inaccurate without the benefit of hard data concerning the expense involved.

I have briefly outlined a proposal for gathering meaningful security cost data and have pointed out the need for it. I have stated and will restate here that through good classification management practices, dollar savings could and should accrue to defense and industry. We, in classification management, must show, with some degree of accuracy, the benefits which are derived from our efforts.

I have developed a survey format which is designed to gather information which, when collated, will provide average base security cost data. This will be distributed to the membership. In the days ahead, we will ask your help in developing a product which will benefit all.

Workshop Leader Green: I think the proposal to conduct a broad based survey of both government and industry is just the thing that we need in order to evaluate classification management as a whole, not that it will identify specific costs, but it will give us at least a bench mark where we can tell whether a program is going forward or is regressing.

I would remind this audience too that we can conceive all sorts of programs, we can initiate surveys, but that these are only a beginning. It is what we do with the result that really justifies the effort, and each of us must give full support to that effort and contribute whenever we can and do whatever we are asked to do.

We tend too much to view our own problems narrowly without fully realizing that others in other disciplines face essentially the same problems. We hear a great deal these days about cost overruns, about escalating prices, bankruptcies, and other fiscal disasters, in both government and industry. One of the major contributing factors must be our failure to utilize some sort of standards for developing and analyzing program costs of all kinds.

I would like to take just a moment and quote very briefly from an article "What Should 'Cost' Mean?" by Robert N. Anthony, the former Assistant Secretary of Defense, Comptroller from 1965 to 1968, and who is now teaching at Harvard Business School:

> Suppose the president of a widget company says, "Last year our cost of manufacturing widgets was $1.80 each." The ordinary person may think he has learned a concrete piece of information from this statement.
>
> Anyone who understands the vagaries of cost accounting knows differently. He knows that "cost" in this context has no generally accepted meaning, that two manufacturers of physically identical widgets who use different, but acceptable, methods of measuring cost could differ in their reported costs of making widgets by 100 percent or more. The informed person therefore realizes that he cannot understand a number that purports to be the cost of a widget unless he knows a great deal about the particular cost accounting system from which it was derived.
>
> Some persons say this situation is inevitable, in view of the complicated nature of business. Others say it is desirable; manufacturers should be encouraged to exercise their own best

> judgment in measuring cost. Still others, including me [meaning Mr. Anthony] find it neither inevitable nor desirable. They [should] find it deplorable.
>
> The increasing number of responsible persons who find it deplorable has generated activity on several fronts to develop cost standards. The activity involves accounting groups, the General Accounting Office, and the Senate Banking and Currency Committee, which plans hearings on the subject.

That is just an introduction to his article. He goes on in great detail to discuss the differences in cost accounting and what impact it has on the government-industry relationship.

I think the interesting thing in his article is that his findings and his recommendations, although much broader in their scope, are similar to those of Art Van Cook: Let government and industry work together to develop and adopt cost standards which will bring about more uniform and realistic charges.

In this Panel, we have attempted to identify several concrete ways in which known costs can be reduced:

One, through a more realistic approach to packaging and shipping. This may require changes in current regulations, which I hope this Society can endorse and support.

We have the means in the present classification management system to provide the detailed component breakdown which we have discussed so often, and which will reduce security costs in the production environment, and we must make better use of this technique.

Finally, in all honesty, it must be said that we have not made great progress since that first Seminar toward standardizing security costs. We still face that larger task of developing those standards.

Art Van Cook has proposed a workable approach which, I think, should be vigorously pursued. We cannot continue to exist as a society, as a community, on theories. We have got to produce some evidence. Our failure to do so may jeopardize the whole future of the classification management program.

Questions and Answers —

Mr. Roy L. Wesley: Roy Wesley, Grumman Aerospace. We are a very fair-sized supplier on Long Island, and I would say about seven months ago — we are participating in the shuttle effort; we have a three-story building that has some 2,500 engineers, and in concert with DCAS in New York, Grumman decided to declassify this building; the reason being we wanted to allow foreign nationals to come to work in a free environment in our facility on Long Island. We did, in fact, by directive declassify this building.

We do not have the dollars to support what we say, but we can identify that we had 250 Sargent Greenleaf locks that cost about $12.50 and 250 five-drawer file cabinets that were used for the handling of classified materials that were returned to us in an open empty condition.

Documents were destroyed. Confidential stuff was eliminated. Duplication was reduced.

We have one floor that has some 35 file cabinets in it that presently contain whatever classified material is required for use in this particular building. We feel that we are going to pursue this effort very diligently at our facility to continue this type of "by direct review" of classified materials. It can be done.

You know, you are going to have some engineers who are going to complain. They are going to say: "Well, it was so convenient when you had it right next to me in my little drawer."

But our management feels that for the

greater good of the corporation and for the entire security system that you can effect savings by taking a very positive action and starting to weed out stuff that you don't really need.

Mr. Henry E. Davis, III, L.T.V. Aerospace: I would be interested in knowing how you treat the item and remarks that say: "Association of production schedules with destination points is classified Confidential, Group 3" — and yet clearly it indicates the rate of delivery is unclassified, the numbers delivered are unclassified. What constitutes "association" and what constitutes "a production schedule"?

Would a shipment of one part going to one destination be significant of anything? Would one part — five parts going to five different locations be significant of anything?

Mr. Buckland: Let's say that our contract calls for a production of 500 of these particular items. That is unclassified. But what they said here is that if we get a call from a certain base stating that they want to have "X" number of these things to go on a specific vehicle at a certain time, that is what we had to classify.

If the destination is not shown, this is fine. But if it is said that this vehicle, stationed at this point, needs this many by this time, that is when "Confidential" is applied because there is a connection to the idea of operational use and military application.

There is a revision to this check list coming out. The end items are going to be unclassified and classification will be applied to protect the military application by not indicating how many are to be shipped to what point, which will give military application.

From the Floor: Would the association of the production schedules that Mr. Pellant would have in transporting those things, would that be a factor that would hinder your traffic department?

Mr. Pellant: There are two aspects in security, as far as transportation is concerned:

One is the hardware itself, which causes its own problems.

The other one is the time of shipment and the time of release and the time of delivery in association with your bigger project or program.

That latter part is the most difficult area in transportation. But the way that is handled normally — that is, providing everybody does what they are supposed to do — is at that point in time the information going to the consignee indicating that it is going to arrive on "X" date by Joe Blow Truck Line or whoever is transporting the material — while normally sent unclassified, should be sent encrypted or classified because then it protects the actual movement.

Now the only deficiency, as opposed to the new procedures under 5200.1, is you are telling the carrier to give signature service, which is telling him he is transporting something at that time. So one defeats the other in actual practice.

Normally speaking, a pre-identification or a report of shipment should be sent unclassified so that it can be handled because you don't normally divulge anything that is classified in it. You say that you are shipping a piece of mechanical gear, machine parts. This is unclassified. You are shipping it by Joe Smith. He is unclassified. It is a bill of lading number that is open to the public. It is moving on a bill of lading number. None of these details are classified.

The fact that the material itself is Confidential or Secret is not classified information until it is related to what the classification of the object is.

So all of these things tend to give you a better flow of intelligence, but if you have also involved the responsibility of maintaining a secure path for the movement, then you run into a different phase of intelligence passing, and unfortunately one sort of counteracts the other, and you get nothing out of it. I am speaking strictly from the transportation standpoint.

From the Floor: Speaking of the transportation, the surface transportation, how would this relate to postal services?

Mr. Pellant: Unfortunately, the mail, the package, when it moves in the postal system eventually finds its way into the commercial transportation system, either in a rail car, in a truck, or in a plane. At that point in time the security procedures of the Post Office Department related to the type of mail services being used are invoked.

If you are shipping first class mail, it is handled expeditiously. Presumably you get twenty-four to forty-eight hour air service on distances exceeding 700 miles. Under 700 miles, under the new postal service regulations, you get surface transportation. And theoretically speaking, it moves very quickly through the transportation system because it has priority rights, and then is delivered the next day by the regular delivery service of the postal system.

As it goes into the postal system, it is maintained and controlled. Once the sack of mail or the shipping container is placed into a commercial conveyance, it is then, as I mentioned, a package. That package is controlled as an inventory tally package for transportation purposes. The contents are not controlled.

If a sack is secure and it arrives secure and it still has the postal lock on it, then you can be reasonably assured that nothing has been taken out. If, however, it arrives without the lock on it, you can be reasonably assured that something may be missing.

But actually you have a little degree of calculated risk, shall we say, in the postal system. It is amazing that this is acceptable, but it is.

Mr. John Gillis, National Academy of Sciences: The discussion today has been more or less restricted to security in the sense of physical security, handling and storage cabinets. But it seems to me that we are falling far short of real cost in classification if we don't start out with the cost of initiating the classification, and also the cost of declassification. I would like to get an opinion from this gentleman as to what he thinks it cost Grumman to go through this little exercise in terms of man hours of effort?

Mr. Wesley: I am unable to give a precise figure. It took quite a bit of time on everybody's part. It took several months, I might add, to get this thing sterilized out.

We believe we have saved in the neighborhood of about $50,000 in container cost and storage and manpower handling of the whole thing just for one little exercise, and we have dumped fifty carloads of material — but I cannot be precise.

Mr. Gillis: The reason I bring this up again, there is a trend in the discussion of some of the other meetings that we lift up the level of classification and have more at a higher level with more input and more consideration before the initial classification is made.

I think merely the exercise that Buckland went through up at Sanders on the reevaluation of the 254 and reworking it, the money spent on that was probably even much greater than he spent on designing the final room here, the assembly here, that he worked on; the man hours of that, the engineers' salaries and wages — this whole area here kind of disturbs me as real cost

that we sort of accepted as part of our day-to-day work but in the real world it is put down there in the cost figures, as Mr. Anthony would like to bring to our attention.

Workshop Leader Green: If we are going to do a thorough cost analysis of the classification management program, we must include in it the cost of classifying and the cost of these reviews that are necessary to determine whether something can be downgraded or declassified.

But I think that our initial thrust has to be to manage those elements of the program that we can by starting out and getting cost figures on known factors. There are so many variables in the decision to classify that it would be extremely difficult, I think, to come up with a base figure, and that was considered in this Panel and the decision was that we would not address the cost of classifying, although I agree with you and I recognize your point that some day we are going to have to face that question of how much does it cost to classify.

From the Floor: Well, the emphasis now again is that everything is overclassified and everyone should start a program like Grumman has started to save these types of costs on shipping, storage, and locks.

But when you go to industry and you raise the point to them, the very first question that they ask themselves is, who is going to do this, and how much is it going to cost in terms of man hours of effort? The figures are astronomical. I think that this is one of the great resistances — people going through their review of their own documents to downgrade them. They just don't have the manpower, and they don't want to spend the money. Somehow, some way, it seems that the government has got to recognize that there is a dilemma here, a cost dilemma — not one of willful not wanting to do the job.

Workshop Leader Green: We hope and firmly believe that the cost advantage of going through this exercise will more than pay the cost of administering it. So we will still have a tremendous cost savings after we have gone through this exercise.

Mr. Van Cook: I would like to give you something on these costs that you are talking about, something that I learned recently. The organization of the Joint Chiefs of Staff undertook in February of 1965 to review World War II documents of Joint Chiefs and Combined Chiefs, policy papers and the like. From the period February, 1965, until April, 1969, a group of reviewers reviewed 240,000 documents at an expenditure of 175 man months — convert that into 13 man years. The cost — and they kept a tally on this thing — was 66¢ per document, on the average. Each document was subjected to three readings — 22¢ per reading was the way it came out. The total cost of that effort was $158,000.

How do you measure that against the value — which is an intangible one — of releasing this kind of information to historical researchers? I don't know how you measure that kind of value in dollars and cents.

However, of the 240,000 documents reviewed, 21,000 were found to require continued classification; 100,000 of them were declassified. Of the 100,000 — 40,000 required British concurrence, which was an effort in itself.

This is the kind of representative cost we can put a handle on. It is the only type of thing that we have.

Let me give you an insight on things that have happened just recently and why we are trying to get these costs. If we find that the cost is so astronomical, we probably should not demand that people all the way along the line be involved in a continuing review process.

In the Department of Defense, records managers advise that — we have in our active office files and records holding areas (temporary storage areas)

12 million cubic feet of records. The best estimate that we can come up with — and this is merely an experience estimate — is that about 15 or 20 percent of these total records holdings are classified. If we say that 17 percent is classified, now that means that we are holding classified about 2,040,000 feet of records.

If one person who is capable of reviewing a foot of records a day for declassification purposes were turned loose on this job, we are talking about 9,200 man years at a cost of about $114 million to review on a continuing basis over a nine-year period.

Put another way: If you took 1,000 people and put them to work on this task exclusively to review these classified records for purposes of declassification over a nine-year period, it would cost $114 million. You will learn tomorrow that the Department of the Army, for example, creates a million feet of records a year, 17 percent of which may be classified, so that over the nine-year period you still have a mountain of additional records to review. The answer to this problem might be to let the records management program take care of it by destruction and retirement and to attack the hill of records in the Archives fifteen years from now rather than the mountain of currently created records.

Mr. William A. Wilson, Air Force Electronics Systems Division: Our problem at my level, the intermediate command level, and I am sure most of the contractors' level, is the proliferation of derivative information. A two-pronged attack is needed:

One is the effort to make the classifier consider the impetus he places on his classification decisions.

And two, putting some meat into the regulation that keeps people from proliferating the information.

Unless we do this, this cost analysis we are making is going to be erroneous. We have got to do it two ways.

Now I have adopted — I see that Mr. Van Cook has upped it; he has got $7.81, and I have been using $6.53 for years. But I found that by using even erroneous figures like this, it gave other management effort in my particular organization the idea that there was a tremendous amount of money being spent by holding classified containers that were not necessary.

We came up with a figure that we, in one small unit, over a period of a year caused the destruction of 20,000 Secret documents and, of course, that is $130,000 we are talking about, if you accept some criterion — and I think we have got to, on a management basis.

Mr. E. H. Stull, Goodyear Aerospace: We presently have a program that is perhaps in its thirteenth or fourteenth year. When the program fist started, the documents weren't marked with the groupings. We have been, every time we come up with one of those, trying to mark it the way it should be. But many of them are group four, but I can't declassify them. They are not subject to automatic declassification — they tell me I can't declassify them, even though they are subject to automatic downgrading.

Mr. Van Cook: You can declassify them if you make a determination that they are group 4 and you have that kind of authority in the ISM. If 12 years old, they would be automatically declassified. You do have that kind of authority, if you withdraw a document from the file that has not been marked, there is a special retroactive provision in the automatic downgrading and declassification system, for you to mark it. If you determine that it is group four, then it is automatically declassified after 12 years.

Mr. Stull: I am told that I must wait for something from the government before I can declassify those.

Mr. Van Cook: No.

Mr. Morton H. Sill, Army Electronics Command: On this automatic downgrading and declassification, there is one other proviso that was brought to our attention forcibly: And that is although it is a group four document, the originator of Top Secret information may place that document into a group three category, therefore, of course, letting it go down into Confidential and remain there. This hasn't been utilized in the past.

Mr. Van Cook: Whether or not it is in the Top Secret category, the original classifying authority may, upon review, determine that the document at some time — let's take a case of a document that was originated eight years ago, and he may determine that now, after a review, that the information should be a group three. We say that is OK, he can do that. He can prolong the classification period provided that he is in a position to notify everybody who holds that information throughout the world that he is doing it, because if he can't — forget it! It is gone; by the automatic system, it is gone.

We had that kind of an experience down at Huntsville, Redstone Arsenal, where one of the contractors, one of the primes on the Nike system said that he is getting guidance today which is putting information in group four that was the same information that was put in group four fifteen years ago. At a meeting with the contractors and the User Agency, I explained to them that if that information was originally group four and the twelve years had expired, unless you can get to everybody in the world who has it and retrieve it, there is no sense in trying to continue to protect it. It is just gone automatically. If it is not practical to protect the information effectively, then there is no sense in tackling it. If it is gone, it is gone. We accept that kind of a degree of risk.

* * * * *

REVIEWS OF WORKSHOPS A AND B

Remarks by Lynwood G. Satterfield —

Last year at Los Angeles, the workshop idea was employed to very good advantage, and the Committee again this year felt that a workshop would be very useful to us. We tried to find two subjects which would be of current interest which we might explore in great detail.

It wasn't through any effort of mine that we had such expert Panelists. I must pass over to Dick Durham and to Bob Green full accolades for selection of their Panel members and for assuring that they would actually do a good job of fitting the things together.

I would like to ask each of them to brief for you their ideas as to what their workshops were intended to develop and perhaps some ideas as to what they thought were developed as a result of their workshops.

Remarks by Richard L. Durham —

In the Lifetime Classification Workshop, we didn't develop solutions; we did develop thoughts. What my experts said suggests that perhaps I could go back now to the drawing board and probably draft a society position paper of some recommended courses of action as a result of what we discussed today.

Jerry Kahan's idea of separation of classification by functional categories, separating out, for example, the political information, the diplomatic type information, from U.S. military hardware information, is one potential approach.

Dr. Lukasik really hit it on the head when he said we really ought to state in the classification guides what it is we are trying to protect. I guess I am going to give an accolade to the AEC. They do a pretty good job of stating this in the classification guide. The only problem is 99-3/10

percent of their classification guides are classified, so you don't really get a chance to see what they are saying.

General Crowson suggested something that — as I mentioned in one of the workshops — something that General Smart of NASA said two years ago, we may need a higher authority. As a slight variance, General Crowson was basically saying, almost at the White House staff level. It is here that inner agency conflicts could be removed.

I think that General Crowson's point was that really you need to get the decision makers at the Assistant Secretary level involved in the classification process and basically they are not.

The time rates that Frank brought up are interesting. I almost wondered if there are people in the audience that maybe could quantify, or some social scientists who could quantify classification. That might be an interesting approach for someone to do a paper on.

I think they all agreed that we have too much that is overclassified, and I think that they basically reached the conclusion, maybe a little differently, that the time has now come — and notwithstanding current problems — to really take a hard look at what we are doing, and try to reduce the problem, try and look at it objectively, from the end of the policy man classifying, the user who is receiving it. If I were a user, that is, a production agency at the bottom, and I didn't understand the reason why it was classified and what I was trying to protect, and I saw that it was costing dollars — I think now that I could get people to listen if I raised the question.

Remarks by Robert E. Green —

This will be nothing but an encapsulation of the things that you heard in our workshop on Security Classification Costing today.

We tried to look at three areas that we felt there would be some chance, some opportunity to identify the elements of cost, and then look at them to see how we could reduce those elements.

And as you recall, we had a very excellent presentation by John Pellant, and I hope that you agree with me now that that forty years of experience has developed a tremendous amount of information that is needed in the classification manual.

The most interesting part to me was that we are dealing with three one-thousandths of 1 percent in dollar values of losses of commodities which might be classified — not necessarily are, but the commodity categories which might be classified, the loss factor is three one-thousandths of 1 percent and only some part of that is classified.

I think that suggests very clearly that we may be paying a great deal of money to buy security protection in the packaging and shipping area for which we get little or no security. The words were used "the anonymity of a package in the transportation system is our best security." The moment we start identifying it by exotic packaging, by banding and seals and that sort of thing, we single it out as a target.

In this area, of course, we are bound by some regulations, and I think that I personally would like to see this Society, if it concurs in this concept, to prepare a position paper, forward it to DoD, one which suggests to them possible changes in the current transportation regulations which will allow us to take advantage of the inherent security in the transportation system and realize some really significant cost savings.

In the area of closed production lines, I am sure that most of this audience knows much better than I all of the various and sundry elements that go into creating cost in running

a closed production line. But the tool to solve that problem already exists. It is one that we have addressed many, many times. It is simply a case of doing what we say we should be doing, and that is, in the preparation of contract security guidance to provide a component breakup for the contractor, an assembly breakdown, so that he knows precisely what is classified and at what point it becomes classified, and then he can plan his production line around that information.

Obviously, if we are going to take the most advantage of cost reductions in this area, we have got to do that at the pre-contract negotiation stage so that each contractor has an opportunity to consider these factors in his bid. This requires no change in regulations. This is up to us individually as classification managers to see that we do in fact consider the component breakdown assembly structure and develop our 254s accordingly.

To parrot Dick Durham's comments, the atmosphere is certainly better now than it has ever been for receiving a contractor's suggestions more favorably than perhaps they have been in the past. There has been a reluctance — and with some justification — on the part of many contractors against "irritating the customer," I think, is the language they like to use, but I think that the atmosphere is better now for that.

Last and by no means the least element we discussed was how tremendous and extremely difficult it is to define administrative and overhead costs, the costs of handling classified documents, declassification, storage, inventory — all of the things that go into your accountability systems, and clearly we have no answer for that at this time. That was recognized years ago and it is still a fact, that we do not have the handle on that type of administrative costs.

I assume — and Art Cook will correct me if I am wrong — that there will be a formal approach from the DoD level to develop the survey that he described so well in his presentation today, to go to representative industry and government activities in a controlled survey, and find out specifically what it costs each of them to handle the same document in the same way, and from that develop that one thing that we need in order to evaluate the classification management program, and that is a bench mark.

Never mind really whether it is $7.18 to handle a document or $5.14, let's have a bench mark from which we can evaluate the program and let management know whether it is paying its way, let it know whether we are making progress or whether we are receding in the program.

We did have a couple of interesting comments that came from questions from the floor that I don't want to overlook in this little summary:

Number one, Jim Bagley pointed out — and it is a very valid comment and it must be considered in any survey that is taken of this security cost — not all activities utilize an accounting system which lends itself to specific costs. Where a contractor is using a very thorough cost accounting system, he can possibly determine some costs.

I can't speak for the Army or the Air Force, but in the Navy where we are using the industrial fund concept, we can identify specific costs, so that the activities selected to be tendered will have to consider the type of accounting system that they have, and whether it lends itself to identifying costs.

There was also mention of a problem in industry concerning the retirement of documents. Industry must maintain accountability for those documents. They may destroy; they may retain. But there is no provision for retirement of those documents, and while they are in the so-called "active" state, they must be fully accounted for, and this, obviously, runs up some rather significant handling costs.

Obviously, there was no answer to that particular problem in this Panel, and it may not really be a classification management problem at all. But the DoD representatives here have indicated that they will take this under advisement and discuss this with the security policy people in DoD to see if there is any possibility to allow a contractor by some means to retire his legitimately retained, but inactive, documents and relieve him of some of the accountability for them.

The one area that we did not discuss — and I think that that is pretty clear why we didn't — is one that we will ultimately have to face. We can talk about identifying the cost of packaging and shipping and handling and this sort of thing but we are not yet prepared to discuss the cost of classifying.

Somewhere downstream, once we have got the handle on these other charges and know what it costs to handle documents after they are classified, we will have a great deal more experience on which we can then tackle the problem of how much does it cost to make this initial decision to classify.

I think that we have several areas here that can be and should be pursued. I think that this Society should support them. I think that each of us, as classification managers, have the means of doing one of them, at least, on our own — and that is the component and assembly breakdown on 254, which certainly is going to help the contractor in planning his production lines.

Questions and Answers —

Mr. Durham: Dr. Lukasik made a remark that seems to me worth repeating:

"You know, I learned more from doing this than perhaps the audience did from me." He said: "This forced me to sit down and take time to look, as far as ARPA is concerned, at security classification, something which I have not done since I have been Director, and something I did not do when I was Acting Director. So," he said, "it was of great benefit to me personally, and I thank the Society for the opportunity."

The Chairman: I think that in a workshop of this kind where we can bring in people who, like Dr. Lukasik, have not specifically thought of classification, they become educated as well as we. And I think that the more that we can do this, bring in people who have the problems of classifying, and get them to thinking about classification, not only do they educate us, but they educate themselves, and at the same time, pass along their ideas.

Mr. Frederick J. Daigle: Fred Daigle, Lockheed. I just would like to get an idea from the attendees:

Most of these people have attended one or more seminars, and even at this seminar — whether they prefer to use a day for workshops, as we have today, or would they prefer a complete series of presentations?

The reason that I ask this, of course, is because we are going to have the seminar on the Coast next year, and we would certainly like to accede to what they prefer in their seminar.

The Chairman: Would you like to have workshops continued at future seminars? The great majority say yes. We would also like you to think about some possible subject matter for workshops, if you are in favor of them.

Mr. Henry E. Davis, III: Henry Davis, LTV Aerospace.

In 1957, the Wright Commission made a rather extensive study of the security program in this country. One of its strongest recommendations that has not been implemented was the elimination of the Confidential classification, and with the very strong statement that in their year or so review, they had not found any Confidential infor-

mation that could incur damage to the country. I would like to know why it has been buried for so long, and why some of the information can't be updated, and why do we keep rediscovering the wheel?

The Chairman: I think I can remember some of the details about not abolishing the Confidential classification.

I don't think a case has really been made, in the first place, for abolishing Confidential.

In the second place, I think that if we did not have a Confidential classification, we would have more information classified at the Secret level. Sooner or later Secret itself would be degraded and then you would find that you would have one classification — in or out.

A lot of people have said that that is not a bad idea. Yet I think that you will all agree that there are items of information of varying degrees of sensitivity, and I think that there are very necessary different degrees of protection that should be afforded to those different levels of sensitive items. I believe that there is room for three levels of classification.

Part of the argument of the Wright Commission was that Confidential receives practically no protection. I don't really quite believe that. I think that if this is so, then the answer is, do we really need Confidential? I would say yes. The Department of Defense says yes. Or should we not rather do a better job of protecting Confidential, making a bigger difference in the way we treat Confidential and Secret and Top Secret?

In the months to come, you will find a great emphasis from the Department of Defense and from the government as a whole, from the President on down, on limiting quite severely the information which is placed in the Top Secret category. And you will also find that there will be considerably greater restrictions on the release and the handling of Top Secret information.

By the same token I believe there will also be greater emphasis on identifying more specifically and differentiating more specifically between Secret and Confidential, and a greater degree of difference in the protection which is afforded to Secret and Confidential.

I don't have any idea of how it will work out, but I do know that you will see some differences.

Mr. William G. Florence, Consultant: I would like to make a suggestion, one that could well be amongst those that you can advise the Committee for a workshop consideration next year.

As the action officer in the Air Force for developing the Air Force position on this Wright Commission Report, I well remember the pro's and con's about eliminating the classification of Confidential.

We had just shortly before gone through the experience of eliminating one classification, and while there was a raising of some information into the Confidential category, speaking affirmatively, there was an improvement in the system as a whole.

Whatever position I might have held back in the 1957 era, I think, had the experience that brings me to agree with anyone who would approach the improvement of our system by eliminating this Confidential designation. We can have different opinions about the relative value of information called Confidential today, and have different opinions about the relative accessibility of that information, or the longevity of that information in that category.

But my point is this: If we could narrow our effort for Secret, narrow it to a decision about what does require protection in the first instance, we would have gone about 99 percent further down the road toward the solution of the problem than where we are

now. I do submit, at the present time, that these little concerns and worries about whether something is Confidential or Secret or not are really beside the point. I think that they take up time and take up expense and that they detract tremendously from really whether something should be safeguarded to preclude its disclosure and to prevent any actual prejudice to the defense of the country.

The Chairman: I think that that is one of our principal interests. Certainly, it is the principal interest of all classification managers to make sure that you do identify information which really, truly warrants protection in the national interest. That is the first thing to consider.

Then I think that the second thing to consider is how sensitive is it, and this is when we get into the levels of classification.

Mr. Van Cook: I just want to mention this, sort of an update on the Wright Commission Report:

Recently, within the past year, Dr. Foster, Director of the Defense Research Engineering, resurrected the idea in discussions with the Defense Science Board, on which Dr. Teller sits for one, of eliminating the Confidential classification.

Dr. Foster, before going forward with the proposal on this aspect, called together the three Assistant Secretaries of the military departments for R&D, and the Chiefs of R&D of each military department, and he asked them to take three major security classification guidances over which they had cognizance — and they included Minuteman, Polaris, and others — and he said: "Consider that we might eliminate the Confidential classification. Tell me what the impact of that would be."

I sat in on a meeting that resulted from this exercise, and to give you an example, the Air Force Assistant Secretary for R&D said that reviewing the guidance, one particular guidance, that fifty-seven items would be moved out of the Confidential category to the Secret category, three items that were originally Confidential might be declassified from a technical and scientific standpoint; however, he couldn't unilaterally act on that kind of a decision; he would have to bring in the operational people to make that kind of a determination.

The same kind of a report was received from the three Assistant Secretaries that were sitting around that table concerning three major programs under their cognizance. As a result of that meeting, Dr. Foster dropped the proposal.

Miriam Rosen, IBM: If Confidential has proved to be that important a classification, why is it we have so little guidance insofar as accountability for it?

Mr. Van Cook: The point I was trying to make is, rather than take Confidential information and put it out in the open, the Confidential information must be afforded some degree of security classification protection. If it has to be given some degree of protection, whatever it might be, we would necessarily have to move it up to Secret, if that is all we have left, if we are not ready to turn it loose.

Miss Rosen: Even in accordance with the manual, there is little guidance to go on as far as accountability for Confidential information.

Mr. Van Cook: But there is some degree of security protection afforded for Confidential.

Miss Rosen: Just an in-and-out measure.

Mr. Van Cook: Yes, but at least it must be safeguarded in some way to give it some degree of protection.

Miss Rosen: But if a piece of Confidential material comes in, someone is assigned to it or signs for it.

The security office or the security people have no way of knowing how many copies may be made and given to somebody else, if there is no accountability record required.

Mr. Van Cook: Well, I guess we have no way of knowing how much Secret material is reproduced and given to somebody else either.

The Chairman: I think that perhaps one of the reasons why there are not accountability records for Confidential as there are for Secret is the great quantity, the tremendous administrative problems that would be involved, and a determination that has been made it is "not worth it." I think this is probably the reason.

Mr. Joseph J. Di Peri: The one thing that I would like to see discussed possibly at the next seminar is an approach to motivating engineers and scientists in complying with the security classification requirements. In other words, some way to arouse their voluntary cooperation in compliance with the requirement to classify information in accordance with the DD 254 additional guidance.

Mr. Durham: I would like to say something along that line: It is a pretty easy thing to do. As Steve Lukasik and Frank Thomas say, if you tell them what it is that you are trying to protect, most engineers and scientific people are going to go along with you. As a matter of fact, they will assist you. They may show that you are in error. They will open up a dialogue. They don't resist it. It is the dialogue that is missing.

From the Floor: It is personal contact that is needed. Create personal contact with your engineer or your scientist, and you will find complete cooperation.

Mr. Green: There is another element too. We have been talking about costs. Offer that engineer an opportunity to buy one more widget through effective classification management, and you have him on your side.

Mr. Victor M. Rosado, White Sands Missile Range: Has the Society ever taken a position on this elimination of Confidential?

The Chairman: No. It has not been proposed to the Society as a possible position.

This is one thing that occurred to me in listening to Mr. Green's comments on the workshops. That is, it would be most appropriate in my opinion — and I endorse the view expressed — for the Society to go on record on various subjects that are developed during the course of the seminar.

Mr. James J. Bagley, NRL: I would like to point out that the Society has, through its own documents, made several points: The Society a year ago recommended that there be a national index for classification.

Two years ago, it was recommended and pointed out in papers that classification is susceptible to systems analysis. The whole body of doctrine, essentially, or positions, if you will, are pretty much contained in our own bulletins.

The Chairman: Certainly there are many positions expressed there that are not necessarily the positions of the people who are members of the Society. There are a lot of points that could be developed, like what is the position of the Society on the elimination of Confidential or on a number of other subjects.

Mr. James D. Moran: I would like to suggest a plan of attack on these proposal items that have come to light in the seminar: The Society leadership should cull these proposals or these suggested items out of the minutes as quickly as possible and detail them on assignment — one to each chapter for development.

President James G. Marsh, Sandia Laboratories: The Board has already

discussed this, Jim, and we are heartily in accord with you. In fact, I was asked together with Mr. Bagley and myself, perhaps we could summarize the possibilities, publicize them in the bulletins, and then ask the chapters to select one or more to work on.

* * * * *

LUNCHEON ADDRESS
BY
DR. HAROLD M. AGNEW

After hearing Kahan and Lukasik and Frank Thomas, it is not clear what is really left to be said on this particular subject of classification and security.

But I must say that I have to commend your Program Chairman George MacClain and President Jim Marsh for all of the things you have arranged, and the papers and things, but when you got the Supreme Court into the act, it seemed that you were going a little bit too far!

As Les Redman implied, almost all of my professional career has been in some way involved in a field which has had a running battle with classification.

I can remember rules that were promulgated at the very beginning of the atomic energy program. There were people at that time, I can recall, who just didn't want to be associated with the program because of classification, but it had some interesting aspects.

Nevertheless, as I mentioned, I have had a running argument on the business of classification security. One ends up sort of saying "Good grief!" But as the recent incidents with regard to the so-called "Pentagon papers" have brought out, in the AEC, at least, the rules have been rather specific, so that the security people, the classification people, have had some basis, let us say, on which to pass judgment — it hasn't been strictly a "gut judgment" all the way.

We have had, of course, senior reviewers, whose attempt in looking at the Act, in their best judgment, is to promulgate essentially proper rules of classification. Once they are in writing, and the classification guides come out, I am afraid that the poor scientists and technicians just have to go along with the system.

To me, it is a little strange that this is still going on today. I believe last year Dr. Teller talked to you on this subject.

I would like to say that in spite of our country's background in freedom, the belief of equal rights, free press, free speech, all the covenants associated with the Constitution, we all know there is today a tremendous amount of secrecy and classification involved in government and in industry. Now some of it is probably warranted and always will be required if we are to have a competitive capitalistic system in industry.

But there does come a time — and this, presumably, was part of the theme in your Section A today — when secrets are no longer secrets, and impedances are really no longer warranted and, in fact, it was pointed out this morning, can be counter productive.

I would like to give you some examples which to me are unwarranted today with regard to classification restrictions. Perhaps some of these may have made some sense at some time but, as I mentioned, I don't think they make sense today and they may have been wrong to impose upon us in the past.

Now, let me start out on a couple of subjects:

One — nuclear weapons in general. Now if you examine the track record from the standpoint of the United States, the Soviet Union, and China — I'm leaving out the United Kingdom and I am leaving out France because there

are certain points which I don't think are relevant to the argument.

But if we look at these three countries I mentioned, we find the following:

For fission bomb development we were first in 1945, then the Soviet Union in 1949 — and I should mention that they were operating at that time from a completely devastated economy, yet just four years after we did, they tested their first fission bomb. And then the Chinese came along in 1964.

And then if I say, well, what was the track record with regard to thermonuclear weapons?

Well, here again — and I am talking about a megaton hydrogen bomb — we were first again in 1952, and then the Soviet Union in 1955, and then the Chinese in 1967. So it took us — and we were first — about seven years from the time we started until the time we got our first thermonuclear weapon, operating from pretty much of a lush economic system, compared with, at least, the Soviet Union at the time.

It did take us longer — and this was brought out this morning — it is the first idea, the first realization, that is hardest. Once somebody realizes that something can be done, then it is a lot easier to attack a problem and to figure out how to do it.

But, nevertheless, it took us seven years from fission to megaton hydrogen bombs, the Soviet Union six, the Chinese only three years. And I think that there is a lesson here that we should be aware of.

Now these developments on the part of the Soviets and the Chinese took appreciably less total time than it took us — and you can say, well, that is because doing it first is harder — but we should keep in mind that all the time that they were carrying out their developments, we were maintaining a very rigorous security system. I think that it is probably one of the best in any particular field that has ever been devised.

I don't believe that these nations received any help from us through the type of leaks that were mentioned this morning, either from the top of the ship or from the bottom of the ship. I just don't think that occurred.

So, I would say that our system cost us a great deal in effort, a great deal of paper work, and a lot of frustration. We did get the job done. But it cost money, and I think that it slowed us down somewhat. But, nevertheless, I don't think it had much effect on the other nations' progress.

Now, I'm not suggesting that physical security of weapons or fissile material is not important. It is extremely important. But what I am trying to point out is that security will not inhibit the development of technology, and secrecy in many instances won't even slow it down.

I strongly believe that once a system is in the field — and I am talking about hardware -- and another nation wants to develop it, it can. Keeping things secret in the sense of the technology and the hardware concepts won't prevent another nation from developing a system and putting it into the field. Now, it may prevent another nation or an individual from copying exactly what you are doing, but he may do it another way. It may be better, or it may be not as good as what you have done, but there are many ways to accomplish a particular objective.

Now let me mention another type of security or classification or inhibition which is really a reflection back to this principle of: "If we keep things secret, if we keep things to ourselves, we will be better off," and as I understand it, your luncheon speaker yesterday gave further examples along this line too.

What I want to talk about is the philosophy of the Battle Act of 1951,

which is really an embargo act. And this particular Act is interesting to read. It includes just about everything, including the kitchen sink — aircraft carriers, even black powder, bombers, scientific instruments — everything possible is in this embargo act.

There are two categories — Category A and Category B:

Category A includes more or less complete weapons systems, such as bombs, tanks, naval vessels, aircraft, and also atomic energy materials. I should mention that the Category A items are handled through military assistance programs.

Category B really represents technology and materials — special metals, berrylium and things like that, and they are handled by the Office of the President, so they can be negotiated if you have got the right ticket — sort of like airline routes; it all depends on whom they are going to be allotted to.

Now, I really believe that our philosophy with regard to these items in today's world is really quite archaic. The nations to whom these embargoes are primarily directed already have a capability of inflicting tremendous damage on each other, or tremendous damage on us. And none of the embargo items are going to change this situation, nor could they conceivably prevent it from occurring. In fact, I would submit that although the embargo concept may have made the attainment of this capability somewhat more difficult for these nations, it has not appreciably affected the time scale with which they achieved this particular position.

If one closely examines the military position of the major nations involved, one has to admit that their conventional, as well as their nuclear capability, is at least on a par with ours.

In fact, around budget time — as I think you are well aware — the Defense Department, our Defense Department argues that their conventional capability in Europe exceeds ours.

Now if the intent of the embargo concept was to guarantee U.S. conventional military superiority, certainly that has failed.

And it appears to me that even our presumed staunchest allies have, from the beginning, traded with the Soviet bloc. I think you remember that during the Cuban crisis, we were putting an embargo on locomotives and trucks, and the United Kingdom continued to sell to Cuba.

I think that you are also aware that Germany's best and biggest trade account, one of the best, is with the Soviets.

Now if you consider the relative military posture of the United States and the rest of the world, of the United States with the Soviet Union and the rest of the world, I don't see any concept of considering continuing this particular embargo philosophy. In fact, since the economic viability of a nation today is probably as important as its strength in military hardware, I believe that the embargo concept, if continued, will really act to the detriment of our country. It may have also been really disadvantageous to us in the past.

Now, I think that there are enough existing federal laws to cover adequately the transfer of items which should not be sold between nations. I think that we have covered that one. For example: Your speaker yesterday mentioned that it was recently carried in a newspaper that we had given permission to the United Kingdom — or "concurrence," perhaps, is a better word — to sell a particular computer to the Soviet Union.

I might say that in Los Alamos, we are continually being asked for advice whether our government should or should not allow the computer companies to sell a computer to somebody in the Soviet bloc. We always say yes. But I don't think those who pose

the question like our answers!

Now, this article hastened to add that although we had given our concurrence, we had been given strict assurance that the Soviet Union would not use it for their nuclear weapons program. Now, I just don't see what difference it would make whether they did or didn't. They have a very credible nuclear force and a nuclear deterrent, and I don't see what difference it makes what they use it for. What bothered me about the whole transaction was that this was a British computer; it was not a U.S. computer.

My feeling was that it should have been a U.S. computer. We need the trade.

Now recently, I think you are aware, the President said that he was going to attempt to open trade with China, and I think that to all of us this was a very good thing to do. But I suspect that all of us, way down deep, said, well, we hope he is going to be careful with regard to what sort of items he allows American industry to trade with China.

I think that we have a built-in fear about trading with a Communist country, which causes us to say: "Well, you can't be too careful in trading with these people." And so, perhaps to satisfy this built-in worry that all of us have, the White House very quickly hastened to add that, of course, we are not going to sell China commercial jet aircraft or diesel locomotives — and then they added that that is really what they want. I guess we all felt: "Gee, that is great; you know, we are not giving them what they want — we are going to sell them a lot of things that they don't want!"

But the point to me is, do we really believe that 750,000,000 people shouldn't have commercial jet aircraft in this year 1971? Do we really believe that they shouldn't have any next year? That they should never have any?

I just think that it is quite clear that if they don't purchase these aircraft from us, they are going to purchase them from, say, France, or from the Soviet Union. And I think that you are aware that the French are coming out with a jet aircraft, an air bus, which is a very good machine and they are selling military aircraft in South America and in Africa. It is just scandalous, I believe, that we don't sell commercial jet aircraft to the Chinese.

Right now our aviation industry is on the ropes. We have developed the technology, we have developed the hardware, but the market is stagnant.

It seems to me that providing China with a modern airline, with the aircraft, the ground equipment, the airfield and navigational aids, would be a real shot in the arm for our whole aviation industry. We really ought to sell what we can. And as I mentioned, if we don't, France with their A300B Airbus will really move in, and we will be out in the cold, and once again the American taxpayers will be taking it in the neck. It costs a lot to do the R&D on these developments and the way you get it back is through sales, and I just think that this is something that we should be doing.

I think that the President is correct in trying to get trade going with China and with other nations. And I think that we as a people should try to help him and urge that we don't hold back on such things as commercial jet aircraft or diesel locomotives.

How on earth is obtaining that type of hardware going to affect the security of the United States? Somebody could say: "Well, they are bringing things into North Vietnam." Well, they are anyway.

I think that we are being a little foolish, and that we are thinking in the past with a philosophy that is absolutely archaic today.

Not long ago, I was in France flying on an aircraft made by Dassault. It

is what we call an "executive jet." I noticed the markings on the aircraft were very strange; they were not in a language that I had ever seen before. It turned out to be Afrikaans. Well, France had made these aircraft for sale to the Union of South Africa but the Dassault representative told us that France could not make delivery to the Union of South Africa because of the following logic of our Commerce Department:

Dassault had designed this aircraft with United States engines. The Union of South Africa, which was buying this aircraft, had no commercial jets. The government was buying these jets, for commercial purposes, but the only jet aircraft in the government were owned by the Air Force.

So, to cut down maintenance problems, they were going to have the South African Air Force service these particular aircraft. Whereupon, our Commerce Department said: "These are military aircraft, and we have joined the United Nations, and we are not selling any of you guys from South Africa military equipment. So you, Dassault, have lost your license with respect to the exportation of these aircraft to South Africa." Well, I don't know how the struggle was resolved. This was two years ago.

But one thing was clear. As a result of that, the French aircraft industry said: "We are not going to buy U.S. engines any more, because you tie our hands. We are not going to buy any U.S. engines. We conceivably will buy from the British or anybody that can make an engine with no strings attached; that is where we are going. We can't tolerate this type of action and this type of philosophy on the part of your government."

And I think that here again it stems back to our fear that if we make something available to someone, it could be bad for ourselves, and I just think that the exact opposite is true in many cases.

Let me mention another subject, a very hot subject that was mentioned this morning. Kahan mentioned it. It had to do with the ABM.

Now one of the requirements of the present system which some of us have questioned, has to do with providing protection against an accidental or inadvertent launch. And that particular requirement imposes some rather strange modifications to the system.

I argue that the way to prevent an accidental or inadvertent launch is at the launch site — not at the target area. We have developed an incredibly fine system of command and control, both in philosophy and in hardware, to prevent inadvertent, unauthorized, accidental launches of missiles.

It seems to me that this particular technology should be made available to any country that has developed an offensive or defensive system. I think that it is just as important to us as it is to them that they don't have an accidental launch.

Now this particular type of technology, unfortunately, is classified. You can't transfer it. But I think that it would really be to our overall benefit if one could have a clear understanding on hardware, command and control hardware, to prevent accidental launches on these types of systems.

Now if we are to do this — for example, if you didn't have this requirement for area coverage which results from protection against an accidental launch, then you could really concentrate on something that I think we are going to do eventually anyway, but we would get to it a lot faster, which is hardsite defense, which could be done in a very credible fashion and at much less cost than one has to provide for if one is providing for area coverage, which you need to protect against an accidental launch.

And in the same context, for the past twenty-four years, those of us asso-

ciated with the Commission have developed very safe nuclear weapons and weapon systems. And I would ask: "Is it in our best interests that systems of other countries should be less safe?" I would think not.

I think again it is to our mutual interests that their nuclear weapons systems be as safe as our nuclear weapons systems against accident or inadvertent or unauthorized use. We have some very good technology. Perhaps the other nations do. Perhaps they don't. But I think again it behooves us to make this technology available, unclassified, for our mutual protection.

You know, sometimes people worry, and sometimes conflict comes out of fear — fear generated by the unknown. I think if you understand a person's system, his command and control system, one perhaps can have a much more stable overall system.

We also classify the yields of nuclear weapons. I don't know why we do that. Within a factor of 10, I don't see that it matters. You could also, you know, really improve the credibility of a deterrent by not keeping such yields secret.

I mean, this was brought out this morning in the context of Japan's technology, very advanced technology, I think, being factual.

There was an era when we even classified the shape of things and we had tremendous tents around our bombs and we tried to operate as if conducting obstetrics under a sheet!

We finally broke that but today the yields question is still with us. I don't see why.

Let me mention, in closing, one more example of unwarranted security. We are planning to detonate a high-yield shot in Alaska. And we have been trying very hard to get, let us say, public acceptance — if that is the right word — to conduct this test in Alaska, and there have been briefing teams going up and down the West Coast and in Alaska and Hawaii and trying to calm people — I think that is the right phrase — and show the ecologists and the environmentalists and the concerned people that indeed the AEC is very prudent in what it plans to conduct, and that they should not worry about this particular planned test.

We announced that the yield will be in the neighborhood of five megatons. But invariably in these briefings, the persons to whom the briefing is addressed ask: "What is it for?"

And they are told it is secret which immediately causes distrust in the people who you are trying to win over. And every time our people go down the drain. Now this is a situation that has been imposed upon the AEC by another authority, but I just think that it is bad politics and it doesn't make any sense.

This morning, I think, it was Kahan who was talking about the need for the public to know. I can't see how, in any way, it would jeopardize the security of the United States to tell the people what the test is for. I think it would make our job of selling the particular test much easier.

You do tests for lots of reasons. Sometimes you build hardware as a result of tests; sometimes you don't. But I think that here is another example of security which immediately alienates the group with which you are trying to communicate and trying to get support for what you are doing.

Well, with that I think I would like to close by just saying that it behooves those of you here in particular to look very closely at the rules that are being imposed upon you.

It was suggested this morning that you might come up with a very clear statement as to why a subject is being classified, you should write down why it was classified instead of relying on all of the sort of arguments that my good friend, Les Reman, has given in the past years that if, well, you don't do this and they think of that,

then they might do this, and so forth and so on.

I would agree that if a weapons component happened to be in the shape of a cube, I would classify it, but any fool would start with some sort of a spherical shape.

Questions and Answers —

From the Floor: The argument that I have heard over and over and over again is that a good deal of classification is warranted on the basis that you are going to have the adversary spend as much money to find out something as we have spent to find it out. And I follow your arguments and I agree with them totally, but what do you have to say on that? For example, they are going to find it out in two years, but if it cost us a billion dollars to find it out, let them spend a billion dollars.

Dr. Agnew: Well, I think that the point is, when you say, "find it out," that is sort of the key. Once it happens, it is found out. I don't think that in today's world that the technology being the way it is, with the number of people in all countries, the number of scientists and engineers that are available, I don't think there are very many bad starts.

It is the concept of having many bad starts where people say then, you know, "you spent a lot of our money because you went down this alley instead of going down the right way," is not true any more. I think that technology has now reached the stage where people can pursue a particular course and get to an objective. It may not be the quickest, it may not be the best, but sometimes you find that perhaps the second best way, being a little more conservative, perhaps, in the long run, is best.

You hear a great deal today about the disadvantage we are in because of our advanced state of technology, of having small systems, which, in a vulnerability sense, are much more vulnerable than big systems. So I just think that technology has reached a stage where the blind path argument is really not around any more.

From the Floor: There has been a discussion this morning about separating political decisions and technological decisions. Being primarily in both fields, would you like to comment on your thoughts overlapping the classification in the political sphere and also in the hard sciences?

Dr. Agnew: Well, I guess, as far as the hard sciences are concerned, once an object is in hardware form, as I said, I think that there is really no more secrecy involved.

In the political sphere, and maybe also in the scientific sphere, when you are making decisions, are you going to do something or aren't you going to do something; for example, say it is a horse race and you know that the long shot is going to win, you had better keep that a secret; otherwise, it is no longer a long shot. It is just that simple. Until you have moved, you can keep things a secret. Once you have moved, I don't think you can keep things secret.

In fact, I have been told by reliable people if I would name a document — they didn't care what it was, that for under $500 they could get it — it didn't matter whose it is, ours, or the AEC or anybodys, there is a system for doing it. So I don't see who it is fooling. So once something is in hardware, that is what I mean by a paper or something, this can be obtained.

In fact, someone was talking this morning about showing the enemy your capabilities. Well, the way you do that, in Vietnam I would say that we pretty much "shot our wad" of conventional capabilities. We have shown everything we have got. The Soviets haven't. Yet we have many things we keep secret. It is just ridiculous, because we are really showing the capabilities of some of these systems in a real world, and that is where it counts.

We don't know what an SA-3 does. They use SA-2's. We don't know anything about SA-5's. They have been very careful in what they have done and we have pretty much "shot our wad," which, I think, is too bad, in an operations sense.

So I think that what is important in the political sense is that up until the time that you choose your option, you should be very careful, but once you have made the decision, once you start moving — and moving to me means putting something in a drawing form or a hardware form or a policy form — it shouldn't be kept classified.

* * * * *

CLASSIFIED RESEARCH AND DEVELOPMENT ON CAMPUS

Remarks of Dr. Edward M. Reilly —

It is a great pleasure to be here with you today sharing the podium with an old associate and friend of the Department of Defense, Dr. Andrew Suttle. I am here today because I have agreed to make a few remarks about defense research in the universities and about our policies regarding the classification of research.

First, let us look at the question of why do we support research in universities. Simply stated, we support it because the kind of scientific and technological innovator who is capable of those radical innovations which provide revolutionary changes in warfare is there. Can one doubt the military importance of Professor Goddard's work on liquid-fuelled rockets today? Certainly Professor Einstein's letter to the President and the ensuing program which attracted considerable university cooperation played a large part in reshaping military technology during the last thirty years and has given us a new needed source of power for both civilian and military use. Let us not forget that the computer age in which we live was born only a few years ago in university research laboratories in Pennsylvania and Massachusetts. The first electronic computer, built for the Army, was used for years to calculate ballistic tables for artillery use. Computers have become so commonplace and inexpensive that today we normally do these calculation in real-time.

Finally, I should mention a university innovator who has produced another technological revolution, Professor Townes; who, while at Columbia, in 1952 developed another interesting idea, the idea of the maser and laser. He showed that there were new ways of stimulating atoms and molecules to give vast amounts of power in parts of the spectral range where we had never had effective power sources. The military support of maser programs and laser programs has become quite extensive in recent years because of their military significance.

At the outset, I might say — to summarize history — we have made these kinds of basic studies in universities and we should constantly support many of them. They do provide a wealth of radical new ideas in science and technology.

For some peculiar reason, radical new ideas and concepts generally do not arise in the industry where one might expect them to arise. Note that the railroad industry does not give birth to an aircraft industry, and the radio industry does not originate a laser industry. Although later on when such technological applications are realized to have commercial value and new industries do develop, they (the older industries) become interested in these newer conceptual ideas.

Another reason these same university graduate research labs are important to us as a national asset is for propagating and spreading these new ideas. We realize today, after having made many studies of defense research, that the value of new technology to the defense establishment is determined not only by the worthwhileness of the idea, but by how fast we can

spread it; how fast we can apply it in our industrial pyramid to many different products and services that have defense implications. And generally, soon after widespread defense application, they have market implications in the commercial and civilian sense.

We need this early application in order to maintain our military posture and really get full advantage of having made this investment in rather basic research.

I might say at the outset that most basic research is characterized by being completely unclassified. It's a characteristic of our scientific adversary system to review critically these new ideas. Basic work is published in the open literature, and, for example, if a Fermi thinks an Einstein is wrong, it would be natural for him to write so in his next publication and say, "You are wrong and here's why." These radical ideas do need a test by other competent scientists, not only in the country where the ideas are born, but internationally, in discussion at the various scientific meetings as well as in the journals. This is one of the main reasons for continuing pressures to keep basic ideas stemming from basic research unclassified and to maintain classification of only their deep implications to defense systems. In other words, they become classified only when they become of great defense importance and have classified ramifications due to other defense information associated with them.

Within the defense establishment and only a few years ago, Dr. Foster issued a directive saying that none of the research at universities supported under our research program should be classified, and the military services were directed to carry out this kind of policy. As Dr. Suttle may tell you, there were inconsistencies that had existed before this enunciation; Dr. Foster's desire was to try to make our support of basic research at universities as appropriate to the academic community as possibly could be done.

Now to put this whole problem of research classification in perspective again, let me tell you one more statistical fact. Even though some 77 percent of our university work is in the category of being supported by a research program and therefore is by definition basic and unclassified, of the remainder only a tiny fraction has been classified because of other policies. One of these policies rests on the need-to-know of our students in our universities who are going to go out and take on new jobs in industry and try to promote new technology. The need for new technological information is very great, and you will find most people with backgrounds such as mine believe that much of our true strength in this country comes from the quickness with which we can train people in these new technologies and the quickness with which we can get industry to produce new and practical military products.

Thus, there is a need-to-know that goes beyond the normal definition of that associated with classification information: the need-to-know in the areas of new technologies. The procurement of up-to-date know-how (by university students) is paramount if we really are to spread these ideas and secure as many applications as possible.

Generally when we classify technology we find its spread is slow and the number of applications is narrowed down to the very few that are under the control of the principal laboratory doing the work.

We all agree, I think, that fundamental or basic research projects really should contain no classified information in themselves, and in fact, most university research never generates any classified information. Most classified information is generated within the defense establishment, and I think that this point needs to be enunciated in connection with the review of papers written in universities. In all the review work

I've done over the years in DDR&E of basic research papers, rarely have I ever found any information that was actually generated in a university to be classified. Generally, what needed to be excised in the review process were those bits of military information that had been unnecessarily added to the paper. And I must tell you again, these have no value in normal scientific literature and therefore can be removed with no harm to the paper in most cases. It is indeed a rare event when military information extracted from such a scientific paper really affects the quality of the paper.

Now, the other way to putting this in perspective is the following. Seventy-seven percent of all university research and development in the country as a whole is basic research. And exactly that fraction happens to be basic research in the group of projects supported by the defense establishment. Some 3,000 of our projects then are by definition unclassified. It is a matter of fact that today there are relatively small numbers of classified projects at universities. At the campus laboratories today we are spending about $220 million to support these 3,000 efforts. We have over the years separated many of the classified activities into special university-operated defense laboratories. At these federal contract research centers that are operated for us by the universities, we are spending over $140 million. Many of these are not even located on campus. The largest two, the Applied Physics Lab of Johns Hopkins and the Lincoln Laboratory at M.I.T., are located miles away from the main campus activities; and these really constitute defense laboratories operated for us with university management. In addition, there remain a few of the so-called think-tanks, most of which have become organizationally or geographically divorced from the universities which originally founded them at defense request. For example, locally, we have both the Institute for Defense Analysis which is now independently managed but came into being because of sponsorship of a group of universities; and the Center for Naval Analysis which is still operated locally for us by the management of the University of Rochester.

At these kinds of special institutes and centers certainly one could expect a large amount of classified defense information to arise, and in fact that is the case. But there has been an honest effort and change in policy over recent years aimed at declassifying most of the science and technology on campus for the reasons that I have tried to describe and place in better perspective for you.

Questions and Answers —

Mr. Rankin (Navy): I would like to address my question to Dr. Reilley.

From the presentation this morning, I gather that there is a feeling that there ought to be a free flow of information not only within the country but with other countries in order to advance research and technology.

I have always been very curious as to whether or not there has been a return of information, especially including the Soviet bloc countries.

Dr. Reilley: I'd say in answer to the question, there has been. As a matter of fact, a few months ago, I had a French visitor in my office. I mentioned to him the tremendous importance that Neel's theory of magnetism had in our defense effort in this country in the development of the magnetic components that go into our computers, memories, and into our microwave radar sets. He said he wished that French industry had realized that contribution in the same manner that we had in this country. I can think of nothing that promoted the rapid advance of applications of magnetism more (in the last twenty years) than this French professor's theory on how magnetic ferrites really work. He gave us the fundamental basis upon which we can now design new materials with desired characteristics. This is one very important

example of an innovation from another country. We had spent much of our time in this country trying to arrive at such a theory, but Neel was the first to do so and he was French.

The interesting thing about this sequence is that the French themselves did not apply this work as quickly as we were able to do. All the work on magnetic materials in this country was unclassified. There was no attempt to classify even the materials that were produced under defense programs.

Mr. Rankin: Is there any evidence from the Soviet bloc countries?

Dr. Reilley: There is much in the literature today to suggest that the true expertise in certain parts of plasma research lies in the Soviet Union, and — to the best of my knowledge — they are publishing freely all their basic work in this field. There is intense interest in America, in our universities particularly, in getting the translations of the pertinent Russian journals just as quickly as possible for that reason. At the moment, they are the leaders and they are openly publishing their work. Recently, they have announced that the head of the leading Plasma Research Institute in the Soviet Union will spend the next year in England working in one of their university laboratories, spreading the word there.

So there is an opening even on the Soviet part with respect to the kind of unclassified basic research of which I was speaking. And we probably will profit by this.

I think you all may know that there was a big policy decision made by our Government some years ago to completely declassify all of the work in plasma physics that might lead to fusion reactors, making cheap electric power really possible. And there is a lot of evidence that the Soviet Union did the same thing and that we are now conversing quite freely with them on the latest ideas and really pushing the state-of-the-art of plasma devices ahead together.

Capt. Taylor (Indiana University): These arguments for supporting classification are among the most logical and the most articulate that I personally have heard in some five years of research in the area of classification management. Why is it that these arguments are not more evident in the scientific and technical literature, and particularly why aren't these arguments disseminated more among those in scientific and technical (fields) particularly in universities such as Indiana where there is no classified research but where the research begets a tremendous amount of agitation and some are very much against any research of any sort?

Dr. Reilley: I suspect (facetiously) part of the reason for the lack of spreading the word is that there aren't any good university courses on this subject.

Seriously though, there is very little training of the general scientific and engineering public in this kind of matter. I think that one of the sad things about the move to remove ROTC from some of our campuses is that at least in ROTC, there was some understanding that came to many of our people of the need for classifying military information (that's where I initially became acquainted with it). That need still exists, along with the newer need of keeping on-campus research unclassified.

Remarks of Dr. Andrew D. Suttle, Jr.—

Whenever one discusses university research and development, the first thing that we often hear now is: What is this doing to the educational program; What is this doing to the undergraduates? I would submit to you that in any research program, not only those sponsored by the Department of Defense but those sponsored by any other group, that we should look at

perhaps four different groups and note their involvement.

First, I think we should look at the faculty members, their research associates, their post-doctoral fellows, and their students.

Next, we should look at the university as an entity. And certainly, we should evaluate the interest of the sponsoring agency.

Finally, since most universities are publicly supported or enjoy tax exemptions, the public interest must be represented and carefully considered.

One thing that we have noticed at Texas A&M University, and that my colleagues throughout the academic world tell me, is that work is only good — it only really gets done well — if the faculty member is interested in it and wants to do it. Therefore, it has been the policy, not only at our institution but also throughout the State of Texas, that it is a part of academic freedom; it is a part of the right of any faculty member, to pursue any project in which he is interested and which the university administration feels we are in a position to support.

Obviously, everyone cannot erect an enormous radio-telescope; everyone cannot have oceanographic vessels; some of our friends, say, in the deep South really are not too well qualified to carry on Artic research. But as long as there is a real need for the work that the university is qualified to provide the facilities for, our test is not is the work classified but is the project of interest to a competent, aggressive, imaginative person.

We are very anxious to engage in the dissemination of information which Dr. Reilly so rightly and properly stressed. The few classified projects that we have had at Texas A&M University have caused us no problem whatever. It is really very easy to strip out what little information may be classified, may be sensitive; and the fundamental test of publication and review by the peers, of the faculty member, and the defense of the dissertation by the student has caused us no problem.

Another way that we feel that we can contribute and participate both in the open and the closed domain is by arranging for faculty members who have research grants and contracts to serve as consultants to various federal agencies, to the various laboratories, or other groups in which the work is closed.

Along the lines that Dr. Reilly was mentioning about the difficulty of classifying material, I think a number of remarks of Edward Teller on this subject merit consideration, although I regret to say I cannot agree with his desire to declassify everything. However, I would, in passing, point out that our nuclear weapons program which has been most heavily classified seems to have received rather wide dissemination through the fact that most of our adversaries have sizable nuclear arsenals; but I understand our computer program which is open to all comers and purchasers is one of those which has been developed very little in the outside world, and that the market for United States computing equipment is one of those which is the greatest.

I think there is a lesson here and that there is some medium between total declassification and the absolute restriction of all information.

Universities are public servants and they certainly have a responsibility to provide education. Education consists in transmitting knowledge which is already known, and also in generating new knowledge.

Research is an integral part of higher education, and research must go forward.

Now, as I look at the progress of Texas A&M University — and it is a land-grant school, one that has grown up to provide education in the agri-

cultural and mechanic arts; and which, if I am not mistaken, the establishing organic act also provided for military instruction, although apparently in recent years this may have been forgotten a little — our original research program was almost entirely conducted by the Department of Agriculture in serving the farmers of the nation. Until the tremendous demands of World War II, almost all of the research in most of the land-grant colleges was through our Agricultural Experiment Stations.

Other research that was done was largely supported by industry, once again through the consulting and research-grant route that we mentioned. I can recall very little discussion and very little objection to faculty members who were consultants to the oil, electrical, chemical industries, being criticized for their consulting activities where the information was available only to their clients, while the research done in their laboratories on campus by their graduate students invariably went into the open domain.

If I am not mistaken, the only institution where this was seriously questioned was the University of Chicago — which was my alma mater — where Dr. Robert Hutchins established two programs: one where the faculty members were free to consult and another where their entire talents were to be devoted to the interest of the university.

So we find that there has been a history of the two phases of the participation by the academic community in providing consultation with limited access to the information while still carrying on their open research programs, the dissemination of information, and the education of graduate students.

A great deal of the objections that we find to classified research, military research, and I might even go so far as to say governmental research, has in my opinion — and we have given this considerable thought at Texas A&M — very, very little to do with the military or with classification. It, I fear, can be laid largely to lackadaisical or rather indifferent management.

Admittedly, immediately following World War II, the several agencies that were supporting research most, the Department of Defense — and I would like here to say a kind word about the Office of Naval Research, which as I understand it was predecessor of the National Science Foundation, and certainly was very good to all universities, ours included — and to the Atomic Energy Commission.

These people had the funds. They were very generous in supporting work. They also had some minimal classification activities that were associated with their efforts. Somehow, government research and classification became, I think largely through lack of clear definition, somewhat entwined.

But actually, the problems and the complaints about sponsored research — and I want to emphasize sponsored research rather than classification — have come from the fact that we in university administration have not exercised our responsibilities. We have permitted individual investigators to work directly and immediately with their sponsors. We have created in some cases almost two classes of citizens: those who are funding themselves, those who fund their own research, and those who rely on the university.

At the same time, as research projects grew and attracted graduate students, faculty members did more research. Fewer of the senior, most able, and brilliant faculty were in the classroom associated with the undergraduates. The graduate students first held laboratories, then discussion sessions, and finally even post-doctoral fellows were teaching lower division freshman and sophomore courses. This resulted in a good deal of unhappiness on the part of the undergraduate students and this has been, I fear, confused very badly with the fact that some very, very small

fraction of the projects that caused this condition or contributed to it may or may not have been classified.

But, once again, let me emphasize that this has been a problem of university administration and management and has in my opinion nothing to do with classification, nothing to do with our participation with the Department of Defense or with the Atomic Energy Commission in particular. It is a phenomenon that applies across the board; it applies in cur relationships with the fine foundations that are our benefactors; it applies to public-spirited industries that have supported work at our institutions. I must emphasize that this failure I think causes much of the criticism that we are now facing.

If we look a little further and consider the real problems of classified work on campus, through cooperation, through your visitors who come to our campus to check our facilities, and their work with our support and administrative people through selection of suitable locations where one does not attempt to perform the little bit of work that was done on campuses in effect in the hallway or in the common; we have found that the mechanics of doing classified work — and we have had four or five projects at A&M — have been very simple.

We have a research annex. We attempt to locate these projects there. We have found that there has been absolutely no problem with maintaining the level of security that is commensurate with the work and with graduating the students who have worked on the programs. We have always welcomed these efforts because we feel that we too have a responsibility to serve the nation and we feel that the defense portion of our nation is one of the most important and is one that we are very happy to serve.

Another point that I would like to stress very definitely is that we at Texas A&M have never tried to conduct classified research, we have never tried to conduct unclassified research, or we have never tried to conduct education under circumstances where the laws of the State of Texas were not observed and enforced.

I think a great deal of problems at universities exist because there are some people who feel that there are special privileges conferred on students. I must say that we feel in the State of Texas in our higher education system that it is our responsibility to maintain conventional law and order on our campuses. This, we feel is a responsibility that we have to the students and is essential to the conduct of our business whether it is education, whether it is research, or whether it is public service.

As Dr. Reilly has indicated to you so very clearly, one of the things that we find far more important than the designation or the sponsor is making certain that the work that is done is a hign quality and that the people who are doing it are very interested in it and that they feel that the work is going to make contribution.

In closing, I would like to stress that we feel in the university world that there is a place for working with all agencies of the Federal Government. We feel that we can collaborate with industry and we feel that our information and knowledge should be current; we should be working in the forefront; and that we should disseminate this information as widely and as rapidly as possible. We should do this by having the most competent people and gathering the most competent students.

We feel that there should be full, thorough, scholarly review by open-minded peers of the individuals who are doing the research. And we have never found any problem in classification in meeting this requirement.

We feel that we should continue to be knowledgeable about maintaining good management, just as you do in government and industry, and avoiding peripheral or extraneous excesses that may reflect adversely on the research program but really have nothing to do

with it.

We would like to say that we are extremely grateful to all of our sponsors and benefactors for their support of our research, and we particularly welcome the opportunity for interchange with them.

I would like to leave on this one note: In the Texas university system, we are far more interested in the quality of the work, the quality of the student in doing a good job, than whether something may or may not be classified.

* * * * *

ARMY RECORDS MANAGEMENT AND ITS RELATIONSHIP WITH DOCUMENT SECURITY CLASSIFICATION MANAGEMENT
BY
SEYMOUR J. POMRENZE

Outline —

A. Introduction

B. Essential of the Army Records Management Program

1. Definition of records management
2. Program priority
3. Records inventory
4. The records "cutoff" concept
5. Records disposition instruction
6. Records control schedules
7. The records holding area
8. The records center
9. Records disposition statistics
10. Records maintenance
11. Files planning
12. Benefits of effective files planning
13. The Army Functional Files System (TAFFS) — An integration of records maintenance and records disposition procedures.
14. Key characteristics of TAFFS
15. Files equipment and supplies management
16. Mail management
17. Access to classified records for unofficial research and freedom of information programs
18. Records declassification — 1945-1961
19. Records declassification — 1961-1971

C. Summary of Army Records Management Essentials

A. Introduction —

George MacClain's invitational letter of 22 April requested me to discuss the "Records Management, Department of the Army, and Its Relationship with Classification Management." He asked me to describe the differences, similarities, and interrelationships between these two programs; how the Army records management program is administered; what it achieves in a scheduled period of time; how documentary records may be maintained so as to facilitate upgrading, downgrading and declassification actions, including remarking and notification, based upon the automatic system or upon individual document review; how to achieve a capability of knowing on a current basis the quantity of classified documents on hand in current files in each of the several levels of security classification.

At this point, I got scared. He surely flattered me if he thought I could do all that. Then I read one more thoughtful sentence. "Of course, in the event that the foregoing does not provide sufficient suggestion, you may feel free to develop your subject in your own way."

Well, I am going to do the latter, with everyone's permission. I am going to stick to the areas where the office that I represent — the Office Management Division, Administrative Services Directorate, TAGO, has the greatest competence — the essentials of the Army Records Management Program — and allow you to draw your own con-

clusions on program interrelationships, techniques on up and down regrading actions, and practical procedures for arriving at meaningful defense document statistics from my rather off-the-cuff comments.

B. Essentials of the Army Records Management Program —

1. Definition. Records management is a part of the field of administrative management and is concerned with records from their birth to their death. For papers that are born, records management becomes involved with the method by which they are produced, the number of copies made and distributed, the marking of papers where required, the movement of papers, filing systems used, space occupied, filing equipment and supplies, files location, filing procedures, training of personnel, and finally disposal or retirement of records.

2. Program priority. In the Army, effective records management began in 1943. The Army Adjutant General was vested with the overall management of just about all areas of records operations. (Reports management is a responsibility of the Comptroller of the Army.) Initially, the program contemplated action on all fronts: records creation, records transmission, records maintenance, records utilization, and records disposition. It became apparent very early in the program that a determination would have to be made as to which of the areas would receive priority attention. This determination was made for the records managers by top-level Army managers. They decided that the single most pressing problem was to get rid of all old files — classified and unclassified because the Army didn't have personnel and space for them. Therefore, we in records management moved into records disposition first — because it was the biggest records problem facing the Army.

3. Record inventory. We didn't know too much about Army records. We, therefore, took stock — made a rough inventory of our records and found out the volume on hand, where the records were located, and what types they included.

4. The record "cutoff" concept. We groped around with the problem and hit on several techniques that are now considered "musts" in records disposition. For one, we discovered that the easiest way to accomplish our records disposition objective systematically was to CUT OFF OUR FILES in block and remove the cutoff files in block from operating offices on a scheduled basis. CUTOFF means the termination of files at regular intervals to permit their transfer or destruction in complete blocks. Under the cutoff process, the file is terminated regularly at the end of a specific period of time or event and a new file is established. You cannot have effective records disposition without this cutoff technique. (I suspect the authors of the DoD automatic declassification system were aware of the Army records cutoff concept when they adopted some of its features. However, the block aspect was seemingly not strongly emphasized for automatic declassification is geared essentially to the individual document.)

5. Records disposition instructions. For cutoff files to move out of operating offices, we developed two tools: records disposition instructions and records control schedules. The first tool involved the identification and evaluation of all Army records by function, subfunction, and process (action, transaction, project) and the development of precise records retention standards. This tremendous job has been completed for nearly all existing Army records — about 1,500 file series. We are continuously studying records created as a result of new functions or functional changes to establish additional records retention standards. (The grouping of defense classification data resembles somewhat the identification of records by functional category. However, the groupings under automatic declassification are too general and conflict too frequently with each other. Also

the declassification periods are too rigid and not geared to specific files series — as the records disposition standards are to specific file series.)

6. Records control schedules. The second, the records control schedule, was a form designed for the management of files, so they would be disposed of systematically. It contained files identification and arrangement information and prescribed the disposition standard applicable to each files series. Late in the 1950s, we decided that we could replace the records control by adopting standardized file labelling. We now prescribe that the label on the first folder of each files series contain in brief information similar to that contained on the records contral schedule, namely, the file number, the file title, the year of accumulation of the file series, and the precise disposition instructions for the files series. Thus, each file custodian quickly knows the content of the file and its disposition.

7. The records holding area. Where was the records manager going to move the cutoff files? We provided two types of facilities to take care of the cutoff files that could not be destroyed in the operating offices — records holding areas and records centers. A Records Holding Area is a facility established at installations and activities in warehouse type space. Low cost shelving and inexpensive cardboard containers are used to house the records that require retention between 2 and 6 years after cutoff, instead of more costly file cabinets, security safes, and other filing equipment. The defense classified and unclassified records in holding areas are controlled at all times and it is relatively simple for operating officials to get out their records in holding areas. The cost of space, equipment, and keeping records in these facilities is considerably lower than keeping them in operating offices — about 35¢ per foot in holding areas compared to about $3.00 a foot in operating offices.

8. The records center. The second facility to which the Army records managers move cutoff files requiring retention for more than 6 years is the records center. The records center to which we move most Army cutoff records is the Washington National Records Center of the General Services Administration at Suitland, Maryland. We also use the GSA Personnel Records Centers at St. Louis for cutoff Army military and civilian personnel folders, and regional GSA records centers and specialized Army record centers for other cutoff Army files. We publish a chart in AR 340-1 showing where we retire specific file categories.

The records center is operationally essentially similar to the records holding area, except that the center is many times larger and is normally located at some distance from the Army installation that it serves. The records center stores defense classified and unclassified records, services inquiries, boils down the records, and transfers the small permanent records to the final resting place of valuable documents — the National Archives of the United States. (Effective block records declassification action cannot begin until the records are older than 3 years. Classification managers should support early removal of defense classified records from operating offices to records centers and concentrate their talents at the record depository level.)

9. Records disposition statistics. It might surprise you to know the percent of destruction we realize in the creating offices as compared to that in records holding areas and record centers. We estimate that of the 100 percent of records that are created in the Army in any one year — usually about 1,000,000 linear feet — we:

— Destroy 78 percent in the current files area within 2 years after cutoff and retire the remaining 22 percent to the records holding area.

— In the records holding area, of the

22 percent we destroy 19 percent within 2 to 6 years after cutoff and retire the remaining 3 percent to the Washington National Records Center and other records centers used by the Army.

— In the records centers, of the 3 percent nearly 2 percent are destroyed sometime within 10-15 years after cutoff. One percent, or about 10,000 linear feet (20,000,000 pieces of paper) are deposited in the National Archives as permanent records.

This is an enviable record — one of the best of any agency in the Federal Government. Such a records destruction achievement for Federal records of agencies heavily laden with defense classified documents would greatly simplify the task of the classification manager.

10. Records maintenance. We had been in the area of records disposition for only a few years when we realized that we couldn't entirely succeed in records disposition unless we licked problems in records maintenance. For example, we could not hope to achieve systematic disposition of records unless we required the separation of permanent and temporary at the time of filing. Also, we could not expect people to move their files as we required them to do, unless the files were arranged in a logical manner — permitting cutoff and retirement. So, we moved into records maintenance to solve problems in that area and to make disposition more effective.

11. Files planning. It was obvious to us we were keeping too many duplicate files at too many files stations. This was not restricted to any particular organizational command nor is it limited to the Army. We also found that the documentation of any one file station was not as complete as we thought it should be. We had large central files which supposedly contained record sets of valuable documents. They more often than not duplicated files maintained by the creating offices, whose files were often found to be more valuable and more complete. We evolved a solution to the problem of duplicate files. It is a Written Files Plan.

Files Planning is concerned with the proper organizational location of files. Just about every organizational element of the Army must have a written files plan which indicates precisely what files are to be maintained and by whom — at which specific organizational levels. (Files planning promotes location of files at point of use in separate files stations.)

12. Benefits of effective files planning. As a result of files planning, we are able to:

a. Reduce the volume of records created by limiting the places where specific files are to be kept.

b. Simplify files operations and disposition. There is less to file and less to get rid of.

c. Increase the accessibility of records. The files are placed where needed the most.

d. Conserve files space. Less files, less file space.

e. Minimize the need for files personnel, equipment, and supplies.

f. Promote better documentation.

13. The Army Functional Files System (TAFFS) — An integration of records maintenance and records disposition procedures. By the end of the 1950s, we became convinced that the several techniques we had developed for effective records maintenance and disposition could be evolved into one comprehensive files management system. This we finalized during 1959-1963 and named it The Army Functional Files System (TAFFS). Its principles and procedures have been adopted by the Navy Department, the Defense Supply Agency, and a number of other elements of DoD — so that today probably a larger percent of DoD records are maintained under functional filing than any other one records arrange-

ment system.

14. Key characteristics of TAFFS. The Army Functional Files System is a system for identifying and arranging Army records to facilitate reference and disposition. Under TAFFS all Army documentation is divided into selected major functional categories and subdivided into subfunctions and processes. Records that document specific actions accomplished in performing assigned missions are thus filed together. Since each organizational element in the Army perform functions, subfunctions, or actions that result in the accumulation of records, it is sound practice to organize the records in these terms — by function, by subfunction, or by action (process). Thus correct files classification of records under TAFFS often requires that the subject of individual documents be subordinated or even ignored in the files classification process. Papers are filed, regardless of subject, under file numbers identifying records that are retained in the office filing the papers — to document its performance of functions, subfunctions, or processes (actions) in carrying out its assigned mission. (In setting up document security classification standards the same techniques should be used.)

TAFFS operates under certain basic principles that simplify record keeping in the Army. Filing and disposition procedures are integrated: they are not two separate sets of actions, as is characteristic of so many filing systems, including the defunct War Department Decimal File System. The file number under TAFFS provides a place where the paper is to be filed, and — at the same time — it also indicates the final disposition that is to be made of the paper. Permanent and temporary papers are mandatorily segregated at the time of filing. This important principle in files maintenance is achieved by placing labels on folders in positions specifically reserved either for temporary or permanent records. Housekeeping and mission records are automatically separated since housekeeping records are grouped under a single major functional number category. The disposition instructions are shown on file folder and file drawer labels, and contain adequate identification and disposition information. One important advantage under TAFFS is that training clerical personnel in record keeping is made easier, since both filing and disposition procedures can be taught at the same time.

15. Files equipment and supplies management. We were concerned with setting standards for files equipment and files supplies almost from the beginning of The Army Records Management Program. We instituted strict controls on the purchase of filing cabinets and files mechanized equipment. We prescribed and enforced rules on eliminating unclassified records from security safes. We issued detailed guidance on the procurement and use of office copiers, security cabinets, and other items of office equipment. We set standards on a variety of items of files supplies — file folders, file guides, file labels.

Many of these pioneer actions have now become widely accepted throughout the Federal Government.

16. Mail management. In the second half of the 1950s, we issued comprehensive standards on handling Army mail operations to correct expensive and inefficient sorting, opening, time-stamping, routing, controlling, and dispatching of unclassified and classified mail operations. We also set standards and procedures in mail messenger operations and in mail pick up and delivery service schedules throughout the Army.

17. Access to classified records for unofficial research and freedom of information programs. The Army Records Management Program was assigned these two programs in view of its concern for expeditious records reference service. The access program became

its responsibility — jointly with the Office of the Freedom of Information of the Office of the Chief of Public Information — as early as 1947-1948. Over the years, a program was developed providing for historical research by unofficial researchers in Army defense classified records — mainly those files in the National Archives and other GSA records depositories.

In 1966, when the Freedom of Information Act was promulgated — effective 4 July 1967 — the responsibility for Army implementation was married with the Army Records Management Program — again as a logical outgrowth of its objective to provide effective records reference service.

18. Army records declassification, 1945-1961. On 17 February 1961, we in records management were assigned the responsibility for records declassification operations vested in The Adjutant General, since we were already deeply involved in the program on access to classified records by unofficial researchers. The Adjutant General had been charged by the Secretary of the Army since 1945 with exercising the Secretary's authority to review and regrade with respect to defense classification all documents originally classified by the Department of the Army and its predecessor and subordinate organizations which may be in the custody of The Adjutant General or referred to him for regrading action.

The regrading function — exercised during 1945-1961 largely on a document-by-document basis — did not appreciably declassify any significant blocks of classified Army records. There was no automatic declassification program during this period, the bulk of the Defense classified records were of relatively recent origin, no significant action had been taken to declassify JCS-CCS documentation or their derivative documentation, little could be done with documents of foreign origin or those documenting foreign policy since the Foreign Relations Series had not yet significantly moved into the World War II era.

19. Army records declassification, 1961-1971. In 1961, a decision was made to concentrate about 1-2 manyears of our declassification efforts on Army classified documents in the National Archives and its related records depositories. (One manyear had to be devoted to specific document declassification review.) Under the Army records maintenance and disposition program, relatively few defense classified records remained in operating offices beyond 2 years after cutoff. During these early years, little would be realized by reviewing these documents for declassification. Also, many defense classified documents would be destroyed under the Army records disposition within 6 years after cutoff and require no declassification action. Most of the remaining defense classified records would be retired to the National Archives or the Washington National Records Center.

The pre-1941 Army defense classified records were studied first and it was determined that essentially all could be declassified except some 200 linear feet of intelligence operational files containing names of intelligence agents and other intelligence methodological data requiring retention of defense classification. The Archivist of the United States was given authority to declassify just about all pre-1941 Army defense classified records, except in the 200 feet of intelligence files.

Functional classification studies were also conducted for the following file series in the National Archives and its related records depositories:

a. General Headquarters, Southwest Pacific Area, Allied Translator and Interpreter Section Publications, 1942-1945.

(1) Bulletins
(2) Current translations
(3) Limited distribution translations
(4) Enemy publications
(5) Interrogation reports

(6) Limited distribution interrogation reports
(7) Spot reports
(8) Research reports

b. GHQ, SWPA.

All war planning documents, 1942-45, consisting of a series of basic outline plans with implementing staff studies, defensive and strategic plans, and related documents.

c. RAINBOW plans.

(1) Operations plans
(2) Concentration plans
(3) Development files

d. Planning documents for projected invasion and occupation of Japan, 1945.

(1) DOWNFALL
(2) OLYMPIC
(3) CORONET
(4) BLACKLIST

e. Coastal and harbor defense planning files.

f. Army Service Forces.

(1) Off, Commanding General
(2) Director of Material
(3) International Division
(4) Director of Military Training
(5) Director of Personnel
(6) Director of Supply

g. OPD Limited Distribution Message Files (Plans and Operations Division) 1942-45, 14 linear feet.

h. Code words used during World War II.

i. ETO and MTO planning documents, 1942-48.

j. Army intelligence decimal files, 1941-48.

k. POW Interrogation files.

This Army declassification program was successful in establishing some meaningful records declassification standards. However, there was a lack of manpower at the National Archives to locate the documents and cross out the classification markings. Thus, a large volume of Army records are declassified de jure but de facto they remain marked classified.

Solutions are being sought to overcome the manpower shortage and to allow the Army declassification program to proceed toward its goal of the 1960s — to declassify all the Army defense classified records at least through 31 December 1945, with very few exceptions.

It might be well to consider action to eliminate the need for physically remarking de jure declassified documents.

C. Summary —

Here are key provisions of the Army records management program:

1. All files must be cutoff in block — to achieve meaningful records disposition.

2. Precise records standards have been established for each files series for maintenance and disposition.

3. Records scheduling data are incorporated on the file label of the first folder of each file series to permit systematic cutoff and disposition of specific file series.

4. Records are moved out of costly operating offices into economical records holding areas within 2 years after cutoff. Those file series that require retention beyond 6 years are retired from the records holding area to the Washington National Records Center or other designated records depository 3 years after cutoff.

5. Very few Army defense classified records remain in current operating offices 2 years after cutoff; and probably over 90 percent of all Army defense classified records are destroyed within 6

years after cutoff.

6. Files planning is applied to all Army files and written files plans are required of nearly all Army organizations. Benefits: reduce the volume of records, simplify records operations, increase records accessibility, conserve files space, personnel, equipment, and supplies, and — most important — promote better documentation.

7. Nearly all Army files are maintained under The Army Functional Files System.

8. Standards have been established for files equipment and file supplies — those used by defense classified records.

9. Comprehensive standards on handling defense classified and unclassified mail are prescribed and generally followed.

10. Improved records reference service is prescribed, including programs to allow unofficial researchers access to defense classified records for unofficial research and to release more widely information and records under the Freedom of Information Act.

11. The Army records declassification program since 1961 concentrated its efforts on setting declassification standards for nearly all Army defense classified records through 1940 and for many Army defense classified records through 1945. These records are not declassifiable automatically. However, little demarking has been accomplished because of manpower shortages.

Questions and Answers —

Mr. Florence· Mr. Pomrenze. You spoke of the relationships of the DoD Directive 5200.9 and its automatic declassification of a certain number of records initiated prior to 1 January 1946. I wonder if you would give us a couple of minutes of your thoughts about the need to improve the type of declassification actions undertaken under that DoD Directive.

Mr. Pomrenze: DoD Directive 5200.9, and its successor, DoD Directive 5200.10 — and their modifications — are the beginnings of comprehensive declassification automatically throughout the Department of Defense. You were involved in the development of 5200.9 and Mr. MacClain and his staff are currently concerned with both 5200.9 and 5200.10. These directives spell out certain types of information that can automatically be declassified or downgraded after it has reached a certain age. For example, group 4 information becomes declassified after 12 years. Group 3, on the other hand, never automatically becomes declassified; it does, however, go down one step at a time after 12-year intervals. Groups 2 and 1 information automatically do not become downgraded or declassified. These directives apply to all information, regardless of the physical form of the record, and they are truly epoch-making documents.

Today, we face a problem somewhat different than the problem facing the declassification managers in 1960. First of all, a decade or more has passed and group 4 documents and information are no problem to us. There does remain a problem with group 1 and group 3 information, which under the two DoD directives still remains classified and is not openly accessible to researchers. Our statistics in the Army show that over 90 percent of the scholarly research requests are for access to World War II defense classified records. These scholars want to see the defense classified planning documents at the higher command levels, the intelligence documents, the political-military documents, the technical equipment documents. Yet, these remain usually CONFIDENTIAL, and in some cases they still carry a higher defense classification.

These are the documents which we have been analyzing to determine how we can declassify them by category. And we have just about finished our studies and are now proceeding to develop specific operational techniques to open to the public just about all of the World War II classified records. Our actions will improve the declassification actions which are not covered by DoD Directive 5200.9, or by DoD Directive 5200.10.

* * * * *

ADDRESS
BY
WILLIAM J. THALER

I spent the first ten years of my twenty-year professional career with the Department of the Navy, Office of Naval Research, and got involved in a tremendous amount of classified work. When I left the government, I reverted to a completely unclassified research project. I have done no classified research for the last ten years. So I thought it would be interesting to share with you some of my thoughts in retrospect of my ten years in one area and the last ten years in the other.

I joined ONR right after I got my Ph.D. in 1950 and started out in the Acoustics Branch, which was essentially unclassified. After about six months, I was loaned to an outfit called the Field Projects Branch which handled all the Navy's participation in nuclear weapons defense. Of course, I had to have a Q clearance and clearances just pyramided after that. I had to take a look at what the Russians were doing in nuclear weapons and that got me in the intelligence category. Nuclear weapons then began to be deliverable by ballistic missiles so I got into the missile detection area, and another set of clearances. I don't want to impress you with all the clearances I've had. I'm sure you have all experienced this situation in your activities.

I would like to say in retrospect though that one thing struck me when I started trying to put some words down on paper. I think that in the ten years I was involved in classified research, when I was actually originating classified documents at a Secret, Top Secret, Restricted Data level, I never once had any specific instructions on how to evaluate the document I was originating as to its classification status. It all seemed to be kind of prescribed by the system. The documents I originated would result from answering some document which came to my desk which already had a level of classification; the reports on the nuclear weapons tests, the very code names of the weapons and the program itself were classified.

I hope the situation has improved somewhat in the ten years since I left, but I wonder whether there really is enough emphasis put on instructing the fellow at the working level as to how he goes about originating the classification.

I began to think then about the general problem of how to get across to you people the message that I feel is the most important thing. Colonel Tanguy touched on it in his remarks. That is to find some way in which to increase public acceptance and understanding of the fact that classification to some degree is absolutely necessary for national security.

I don't really think that the climate today permits us any longer, as some of the previous speakers just said, to say it's in the best interest of national security and whether you agree with it or not just accept it on face. The generations that are here now and that are coming up are not going to accept this kind of admonition.

It turned out as far as I'm concerned, when I left the Navy I had to make a decision when I went to the university as to whether I should continue classified research or not. It's a hard question. When you're an academician you get paid for nine months of teaching and in the three summer months, you either get research grants or consulting or you don't eat. When you have contacts, it would have been easy to get classified research. But I thought it over carefully and decided, and I still feel this way very strongly, that classified research has no legitimate role in the educational function of the university.

The dilemma there is how can you make available to the national security interest the tremendous talent that lies at all of our universities, the faculty and the students as well. I just simply decided that I didn't want to be involved in classified research at the university. I did do some consulting occasionally but once you get out of the circle and don't participate, you just kind of scale off over the years. I've had just as much fun in unclassified, maybe more, than I did in classified, so it didn't bother me a great deal.

The theme of your seminar this year is Realistic Management of Security Classification in Research and Development. Over the twenty years that I have been in that game, lumping research and development together in just kind of a big mass, or a big morass I guess you'd just say, is a dangerous thing. I would feel compelled to divide research into basic research and applied research; and the development, the hardware, into systems.

Basic research is the cornerstone on which our progress in science and technology lies. I do not believe it's possible to find any significant advantage from the national defense standpoint by classifying basic research.

At the same time, I'm convinced it's absolutely necessary to have the capability of maintaining security classification in applied research and development in certain specific areas where our survival as a nation depends upon depriving a potential enemy of detailed information on our state of readiness to defend ourselves.

It seems to me that the ideal situation of a completely totally open society is not likely to be realizable in the foreseeable future. Unfortunately, even though the present climate of isolatism in this country seems to be growing, it is an inescapable fact of life that there are nations that do in fact seek to dominate their neighbors by subversion, by the threat of force, and as we have seen in Hungary and Czechoslovakia by actual armed intervention. The underlying reason for the continued existence of a body of classified information is to safeguard the security of the United States.

I don't believe this message has been made clear to the American people. Perhaps your organization should broaden its perspective and instead of providing a forum for talking to one another, you should attempt to educate the general public so they will understand and support your activities. In fact, I feel I should be extremely positive with these remarks about the need for improving public relations.

Science and engineering are suffering right now because of a lack of understanding by the general public which has led in fact to a falling out of favor of scientists and engineers. In my opinion and based on some recent data that has just come out this month, it will be about ten years or so before the public and certain elected officials realize that they literally cannot live without us — at least not in the style to which they have become accustomed. I believe it's also true that we literally cannot live as a nation without a certain minimum amount of classified information.

It is obvious that there are certain elements of the government that dread any limited confrontation with the Soviet Union and now Red China because it may lead up the ladder of escalation to nuclear war. It permeates so much of their thinking about world affairs, and more and more in recent years it has tempted many of them into an escapist postulate of a world enforced by love and mutual forbearance. That's a great platitude but it just isn't practical.

Much of the agonizing about Vietnam right now is due to our early and our present fears of escalation which essentially have dictated a no-win policy there. We have been at the peace table in Paris for over two years now with nothing but fancy rhetoric and fierce propaganda. Significantly enough we are now hoping for closed "secret or classified" meetings to achieve a mutually acceptable settlement. The SALT talks have been going on for two years now, another attempt to negotiate disarmament; and while they talk again in "closed," "secret" meetings, the Soviets continue to increase their military superiority and we continue to cut back in our national defense effort.

The fact of the matter is the American public is separated from the truth by a web of secrecy and every so often there's a break in the web and we have a Pentagon Papers incident. Then old secrets are served up to us with endless interpretations pro and con by the press. Once the press gets hold of something like that, it's amazing what a variety of interpretations can be placed on the information. One is almost tempted to believe that the secrecy is maintained because no one could possibly decide which interpretation is in fact correct.

I hope I have established the point that some degree of secrecy is required. There must be some body of classified information whose security must be maintained. The difficult question is who is going to decide which areas should be classified and what specific information within these selected areas will be classified.

You are all well aware of the diversity of interests which practice classification. I sat down when I was trying to write this paper and tried to write a list of all the areas across the spectrum that practice classification as a necessary evil. And you can't think of an area that doesn't involve a classification: the political area, the industrial area, the military area, the diplomatic area, and on and on; and then when you subdivide this, the list is endless. I finally just gave up on it.

Your organization, in my opinion, if it's to be anything more than a group of caretakers of documents had better begin wrestling with this problem of who decides and what areas and what specific items within an area should be classified, if you haven't already begun to do this.

Perhaps you could find it profitable for yourselves and for the country to espouse some of the innovative ideas, for example, the one that John Foster of the DDRE proposed in April of 1970, where essentially he said, you really can't protect R&D information by classifying it for a period in excess of 2 years. And so he proposed that in fact you raise the security classification to Secret. This is essentially saying let's get rid of the Confidential just as we got rid of the Restricted category in 1953. At the end of the 2-year period, you automatically declassify unless there is some overwhelming reason shown why that information can't be declassified. Needless to say, his proposals haven't been accepted. I am sure there are people among you who violently oppose such an incursion on your prerogative.

Perhaps that's not a good idea. But I hope some of you are thinking seriously about some ideas which are practical which can be proposed and can be made to work. I thought about it over the past week and I'm sorry I haven't come up with any magic formula. The systems requirements are

so complex that it will require considerable study. And I think one of the major features of your organization is that you have the talent within house to do this kind of study and to try to make an impact on your superiors and the people up in the higher levels of government, both executive and military branch, that decide these policy matters.

I'd just like to close by reading the final section of the Foreword in a book that I helped to write as a matter of fact. I got involved about 1969 in the ABM controversy and I felt very strongly that the ABM system was a necessary system for the preservation of our national security. And so Dr. Libby and General Twining and myself co-chaired a panel of experts who went through all the unclassified literature we could find and wrote our conclusions. The book has been printed.

I think one of the underlying reasons why we wrote that book was an attempt to get some of the facts, most of which are buried deeply in the classified literature, to get the exact precise facts, but many of which we were able to dig out from unclassified, almost all in fact if we looked hard enough.

And that section of the Foreword is entitled "Public Need to Know":

> The practice in the Department of Defense and the intelligence community has been to classify information about the USSR's capabilities and intentions even though the Soviets know that the U.S.A. already has the information.
>
> Official secrecy concerning our knowledge of Soviet capabilities is supposed to be justified by the need to keep information from potential enemies.
>
> There are areas where secrecy is necessary. Unfortunately, however, we have carried secrecy to the point of obsession, and this obsession has frefrequently been far more successful in keeping vital information from the American people, from Congress, and from our allies than it has been in keeping it from the Soviets. But perhaps the greatest consequence of excessive secrecy is that it undermines the democratic system, because democracy simply will not work if the people do not have the essential facts.
>
> This is dramatically demonstrated by the current debate on the ABM — I might say this was written in '69, and the debate is still raging — because there is no question that the administration has been handicapped by public ignorance of some of the vital facts about the growth of Soviet strategic forces.
>
> Secretary of Defense Melvin Laird is making a start towards bringing the klieg light of truth to bear on our actual national security situation.
>
> This change in policy has been handicapped because some of the hard truths contradict the all-is-well impression given by his predecessors. Some may argue that the frank and forthright testimony of Secretary Laird, Deputy Secretary of Defense Packard, and Chairman of the Joint Chiefs of Staff General Wheeler showed up some of the critical weaknesses of our defense posture and reveals some heretofore classified intelligence information. But the strength of America and its free institutions has always resided in the public understanding of the issues and problems that confront our representative government.

I hope that your organization has the courage to lead the way to more enlightened classification philosophy and doctrine which will provide the American people with the information they need under our democratic system to make the right decisions which are necessary to preserve our national

security.

Questions and Answers —

Mr. Uhland (General Electric, Philadelphia): Professor Thaler, since your participation on that panel with that group, have you changed your mind about the ABM?

Dr. Thaler: No. I very definitely have not.

I really cannot understand in the face of all the historical evidence of the past two decades, how anyone could rely on the good faith and forbearance of the Soviet Union. I'm sorry — I don't want to be a hawk. But I don't want to be dead either. And I am absolutely convinced that if they ever obtain significant strategic military superiority, they will no more hesitate to use that against us then they hesitated to use it against Czechoslovakia and Hungary.

* * * * *

THE RAVELLED THREAD
BY
DONALD B. WOODBRIDGE

As I contemplate my predicament here today, I can't help thinking about a cartoon I saw in the New Yorker some years ago. The scene was one of those rug-sized desert islands so dear to the cartoonist's heart. On the island, besides the inevitable solitary palm tree, were a pretty girl, just out of her teens, in a becomingly tattered dress, and a young lad of eleven or twelve in full Boy Scout regalia including hat. We see him busily engaged over a cooking fire, while all around him we can observe the results of his untiring efforts — a lean-to, a clothes line with clothes a-drying, fish traps, baskets of shell fish, racks for drying fish, a rig to catch water, and I don't remember what else. Our pretty girl in her pretty tatters looks on admiringly, and in her admiration is inspired to exclaim: "Gosh, Roger, I sure was lucky to be cast ashore with a boy like you — I guess."

And so today I can exclaim: "Gosh, fellows, I sure am lucky to be cast ashore here at the Hilton with a ready-made captive audience, eager to listen to my words of wisdom and my badinage — I guess." Not long ago, I was looking forward, peaceful and relaxed, to being just one of the listeners at this seminar. I watched with satisfaction the various spots on the program fill up under George MacClain's skillful maneuvering and then -- ZAP — something happened and here I am cast in the role of a luncheon speaker. The origins of good fortune — or bad, as the case may be — are often obscure, hard to find, maybe legendary, like the sources of the Nile. To whom am I indebted for this turn of the wheel? It's not really George MacClain and Lynn Satterfield — they're caught in the same whirlpool, the same maelstrom that cast me up here on the rostrum. Do I owe my thanks to Daniel Ellsburg, Arthur Sulzberger, or Hugo Black? Or are there secrets still in the Pentagon, unknown to the TIMES and me, that might shed light on the origins of this involvement? If there are, does not NCMS have the right to know? Is it not the patriotic duty of the NCMS Bulletin to publish them?

It occurs to me that with this apotheosis to the Olympian heights of the luncheon speaker it has been my privilege to address the Society in just about every capacity these seminars offer. That the Society has tolerated this confrontation for seven years is an example of unparalleled and astonishing generosity for which I am truly grateful — and there is no guessing about that. Since I, too, am now self-employed — to use a phrase made famous during this seminar — and this may well be the last time I address you — I am going to speak to you as Don Woodbridge — not as Counselor of the Society, but in very personal words. This is not a

position paper.

Early this June, Nora and I took a sentimental journey back to Amherst to join my classmates in the celebration of our 45th reunion. A most interesting experience — an opportunity to see what had happened, in the almost half century, on the one hand to my classmates and on the other hand to the youth of the land as embodied in the undergraduates at a so-called small New England College. (Compared to the enrollment of my day Amherst is hardly small any more.) As I remarked to Nora, it was rather like visiting a foreign land and watching the natives going about the business of working, playing and loving. Loving had picked up a lot since my day with the invasion by female students. I am happy to report that unisex does not appear to have taken root on the campus. Girls can be recognized as such. Their hair is usually at least twice as long as the boys' hair, they favor miniskirts and microskirts — especially when they have good legs — and even when they wear pants and jeans, certain anatomical differentiations persist in manifesting themselves. But it remains a great mystery to me why those young ladies go to such lengths to conceal their natural attractiveness — except in the matter of legs.

As for the boys, once I got used to the long hair, they did not seem basically to be too much different from boys I had known long ago. What's more, they were polite and cheerful. And in the evening when they drifted into our reunion tent, the generation gap seemed to close up a bit as they joined in singing the old songs, the sentimental songs, the songs of simple-minded loyalty — singing as if they meant it, too. And their voices were better than ours.

During commencement week the college offers an afternoon of intellectual fare of a reasonably digestible sort in the form of a trio of lectures presented by three of the abler and more entertaining professors who have been drafted for the occasion by means not shown. There was a talk on the Greek idea of form with the provocative title, "Pots and People." Over in the new music building with its anechoic recital hall we were treated to a musical detective story about Mozart's unfinished mass in C minor, embellished by illustrative musical passages reproduced for us on the most up-to-date sound equipment. Then there was Peter Fischer's discourse on writers in politics. He, too, had a whimsical title — or rather subtitle — "Norman Mailer's Dream Come True — Sort of — in Russia." Professor Fischer is of Polish extration and feels strongly about the importance of Russian studies in American colleges. He worked into his subject rather obliquely (as I am working into mine) by bemoaning the lack of funds to finance an extended field trip into Russia planned by a select group of his students for the mid-term break; and to lend humorous point to his lament about how little we know about Russia and how much there is to learn, he gave us excerpts from the mythical Radio Armenia, a radio station that exists only in the stories that circulate in the underground. Radio Armenia runs a sort of question-and-answer game, sort of like Dear Abby, except that it is political. I am annoyed with myself that I can remember only a few of the questions Professor Fischer amused us with. I should have taken notes. First, there was the inquiry: "What is the difference between capitalism and socialism?" to which Radio Armenia replies: "Under capitalism we have the exploitation of man by man, under socialism the situation is exactly the reverse." Another "correspondent" wants to know what would happen to the economy of the Sahara under socialism. Radio Armenia's answer — "In two years they would be importing sand." That gives you an idea about Radio Armenia. (I'm saving a third story till later.)

As a further illustration of the gap between the Russian mind and the western mind, Professor Fischer gave us an extraordinary account of the final

rounds in the hockey contest at the last Olympics. The four teams left in the running were the United States, Sweden, Russia, and Czechoslovakia; but only the Russians and the Czechs really counted as finalists. The Americans, loyal to the amateur code of the Olympics, fielded a teamof college boys, but the East Europeans were not hung up by any nonsense about the difference between professionals and amateurs. For them, sport is an extension of politics. The Czechs were thought to have a slight edge. What happened? In the next-to-last round the Czechs let the Swedes and the American beat them by ridiculous margins. Western sports writers called it a slump. The Russians were not so sure. They hoped it was a slump, but found out it was not when the Czechs held them to a tie and then in the final round defeated them overwhelmingly. It was quite apparent to the Russian sports writers and the Russian sports fans that the Czech performance was a political act. By letting the Swedes and the American college boys beat them (thereby forfeiting the championship) and then going on to crush the Russians, the Czechs were telling the world in one of the few ways left open to them what they thought of their oppressors. But the West failed utterly to appreciate the extraordinary drama that was being played out on the Olympic ice.

And now I remember another Radio Armenia story. A questioner wants to know why Russian soldiers are staying so long in Czechoslovakia. "Because," says Radio Armenia, "they are still trying to find the people who asked them to come in the first place." I hardly need to point out that Radio Hanoi or the New York Times might happily plagiarize this anecdote.

All this, I say, was by way of leading up to the main theme of Peter Fischer's lecture: the writer in Russia as the conscience of the people. The theme is not new, of course. A cover story in Time back in September of 1968 was devoted to it. On the cover was Solzhenitsyn, generally regarded as Russia's foremost writer today. Solzhenitsyn was the hero of Fischer's story, too. It was in 1962, you may remember, that Solzhenitsyn suddenly became famous, not only in Russia, but throughout the world, with the extraordinary publication of his short, biting novel of the prison camps, "One Day in the Life of Ivan Denisovich." Extraordinary because the publication was not merely authorized, but commanded by Khrushchev himself as part of his campaign to destroy the image of Stalin. After Khrushchev's removal from power in 1964 the brief spell of sunshine for Russia's writers rapidly gave way to darkness again, but the memory of that sunshine and the ferment could not be extinguished. Solzhenitsyn continues to write. His "Cancer Ward" and "The First Circle" have become famous along with Ivan Denisovich. How could that happen when all publication was banned? It is the famous samisdat, the self-publishing carried out by thousands of Russians in privacy and secrecy, copying entire books, laboriously, one copy at a time, chain-letter fashion, till the number of copies of a book like "The First Circle" becomes many thousand and copies find their way to foreign lands and the publishing houses of the West. Thus, the writer in the totalitarian state becomes the conscience, the rallying point, the hope of his countrymen. A character is "The First Circle" makes this telling remark:

> For a country to have a great writer is like having another government. That's why no regime has ever loved great writers — only minor ones.

Solzhenitsyn might be speaking of himself.

Where does Norman Mailer fit into this picture? I suspect that Professor Fischer does not approve of Norman Mailer. Mailer, he thinks, aspires to the role of America's conscience, to be a Solzhenitsyn of the United States. But in this country Mailer's

voice is just one among many voices trying to rally men to this cause or that, with nothing standing in their way except their own lack of eloquence and appeal or perhaps their stupidity. There is not even prior restraint. Peter Fischer would advise Norman Mailer to move to Russia, if Norman seeks that kind of fulfillment.

It is instructive to keep the picture of the Russian writer in the Russian terror state in mind as we contemplate the battlefield of the Pentagon Papers. I suppose that is the name that will stock and be carried on in the history books, though McNamara Memoir and Rand Review are equally alliterative and more precise. But by attaching the papers in people's minds to the Pentagon you can spread the notion of guilt and conspiracy much farther, and that is what most historians are going to want to do — at least in the near future.

In a country like Russia, having a great writer is like having another government, says Solzhenitsyn. In a country like America, having the Fourth Estate is like having another government. Or the Fourth Estate might be said to be the fourth branch of government, introducing another set of checks and balances to interact with the executive, legislative, and judicial. The influence of the press and television, the purveyors of news and nonsense, upon the executive and legislative branches has long been accepted as salutary; some would say indispensable. Do we have evidence now that the checks and balances exerted by the Fourth Estate are having their effect in the judicial branch?

As the power of the Fourth Estate grows, so does its arrogance. Arthur Sulzberger and his fellow conspirators would have us accept the image of their actions as courageous, patriotic, sacrificial, the beginning of salvation for this country. They may be all that, but it does not take a very drastic shift in viewpoint to see them as an exhibition of colossal arrogance and a calculated power play. Deceit, mendacity, and conspiracy are not the exclusive stock in trade of any single institution.

And now I think it is time to give my last broadcast from Radio Armenia. A very unusual question has just come in. "Suppose," says our correspondent, "that as a new departure in diplomacy, a new effort at detente, the governments of the U.S.S.R. and the United States arrange for a foot race around the Kremlin between President Nixon and First Party Secretary Brezhnev; and suppose further that President Nixon should win. How should this be reported in the Russian press?"

"It should be reported as follows," replies Radio Armenia: "In a recent athletic contest consisting in a race around the Kremlin, Comrade Brezhnev was in excellent form and took second place. President Nixon, who was among the contestants, came in next to last."

How different are things on this side of the iron curtain? One thing is sure; we are a long way removed from the solitary writer-hero standing alone as the conscience of his countrymen and vulnerable as hell.

I keep wondering what my attitude toward the Battle of the Pentagon Papers and its chief protagonist would be if I had not spent nearly 30 years of my life in a business where secrecy was a way of life and if some ten of those years had not been closely connected with classification. I do not feel that my life has been narrowed or my soul warped, or that my character has turned sinister. And I have the conviction that I have served my country in an area crucial to its survival and that the country I served deserved to survive — in spite of mounting evidence to the contrary.

And the secrets we kept, at least as far as my business was concerned, deserved for the most part to be kept.

If you are like me in this matter of the Pentagon Papers, you feel an urge to close ranks, to rise to the defense of your profession. The sense of outrage is strong, but the nature of this outrage is quite different from the outrage expressed by certain Congressmen. I think the root of our outrage lies in our having to face the fact that the ultimate ground of our security has been breached and that the man who admits to that breach is being glorified for it. The ultimate ground of our security is, of course, the integrity of the individual men and women to whom we entrust our security — integrity and the sanctity of their pledges.

And so we come face to face with the age-old question: in what level of hell, heaven, or purgatory shall we find the traitor who betrayed his trust for a noble cause? Christian theology leads us to believe that it was necessary for the fulfillment of God's plan that Judas Iscariot betray his Lord. But it was Jesus who was glorified, while Judas remains for all time the archetype of traitor. Is Judas now in hell or heaven?

Perhaps it is necessary for the rebirth of this country of ours that the secret places be aired and that the whirlwind sweep through the corridors of power; but does that make the man who breaks his word, betrays his trust and violates his pledge any less a traitor? To whom are we willing to entrust the decision that a cause is noble enough to justify treachery in its behalf? When we say that the end justifies the means we assume the prerogative of deity; we assume that we know God's plan. I think that is a dangerous assumption. Let me read you a question from my talk at the 1968 Seminar in San Francisco.

"Will the day come when a great physicist, a man of surpassing intellect, moved by great compassion, undertakes to play God for the rest of us and decide which apples from the tree of knowledge we may eat? It raises an interesting question: should the instinct to play God be grounds for denying security clearance — like the instinct for throwing stones at glass houses?" Back in '68 I had different circumstances in mind, but in retrospect the words have a certain prophetic quality.

The basic fabric of society does not consist of governments and institutions, capital and labor, industries and the press; the basic fabric consists of the threads that tie its individual cells together, the bonds of love, affection, cooperation, confidence and trust that tie one man to another, a man to a woman, you to me. When these threads start to ravel the whole fabric is imperilled. Fortunately, the fabric of society, being organic unlike the garments we wear, has extraordinary regenerative powers — up to a point. Let us hope, ladies and gentlemen, that we are not witnessing an unravelling that will pass the point of no return.

* * * * *

THE IMPACT ON NATIONAL SECURITY CAUSED BY RESTRICTIONS ON DEFENSE RESEARCH AND DEVELOPMENT INFORMATION

BY
COLONEL ROBERT B. TANGUY, USAF

After some introductory remarks on my paper, I'd like to give a brief outline of it and follow that with the main conclusions and recommendations and then give a few summary remarks.

This paper addresses the Federal Government's withholding and disseminating defense R&D information and the impact that this has on our national security.

Work was started on the paper in August 1969 at the National War College and completed in the spring 1970. Since that was over a year ago, there are some things in the paper that have

been overtaken by recent events. The paper served as my Master's thesis in Political Science at George Washington University, and has been released by OSD for publication in the National War College Forum.

I examined a dirth of information on this subject, which included all the Congressional committee and subcommittee hearings that were pertinent.

Many of your colleagues here gave me considerable assistance — Dick Durham, Mr. Bagley, Mr. MacClain and Don Garrett.

I started off with an introductory rationale: that we have had in the past several years, since World War II, a great explosion in the R&D information area and this has changed, significantly, the classification of material in the government.

After a general development of the DoD system of withholding and disseminating information, I presented a history of the security classification system, the statutes and Executive Orders associated with that history. I also described the system of limited and unlimited distribution. As I began to get more and more into that area, I realized it was a very significant one, that is to say, the handling of limited or unclassified distribution of information.

Then I addressed what I considered the main issues concerning the system. I examined the citizens' issues, that were being raised. They generally were issues of freedom versus secrecy in our society. Issues raised by the academic and scientific communities were covered as well as those of industry. I included briefly the issue of manpower and equipment costs — direct and indirect costs in dollars.

I assessed, so to speak, management, concentrating in the area of restriction of unclassified information.

The four major conclusions that I drew were: first concerned the statutes and laws. Although I've lived with the classification system as an officer in the Air Force, I was absolutely amazed at the statutes that are involved in constraining government information. They are far too numerous, unclear, and in many instances just downright impractical. The Freedom of Information Act, although certainly not a constraint, as far as I am concerned does little more than recognize Executive Order 10501 and all the other statutes that restrict information. Although this Act places the burden on government to show why it must withhold a document, it is too expensive for most citizens to take the government to court for a document or a piece of information. The Congress should take immediate steps to make a sweeping examination and a reevaluation of the multitude of statutes that are on the books concerning the restriction of information today, to simplify, clarify and make some useful laws. I feel that this would really help you people, the government, the executive as well.

Conclusion number two: That, although they can be made tolerable, there are certain inescapable penalties associated with restricting scientific and technical information. This is rather obvious, in a way, but I think it's something we all should continue to remember, all of us that are in the management business from top to bottom.

Although science and technology obviously have flourished under the constraints of secrecy as evidenced in Russia, Germany and in the United States during World War II, there is adequate testimony on the Congressional books today by some very responsible people and evidence to conclude that in a democracy restrictions to the free exchange of knowledge has and will continue to inhibit free men.

There came to me a strong sense from

going through this material that the psychological effects of secrecy, particularly in the academic community, is costly to scientific research in this country.

Under this conclusion concerning penalties, I stated that the direct and indirect costing in terms of manpower, equipment and money to initiate, handle, and maintain classification material is terribly expensive — and this information was rather limited. These costs can be minimized through the kind of work that you people as a Society are doing. I specifically stated, the efforts of the NCMS through its regular meetings, seminars, journals, and bulletins are an excellent example of the kind of action the government needs. You need ever-increasing backing.

Conclusion number three: There are certain management aspects of the systems that are significantly increasing the penalty. These concern the limited distribution constraints. During preparation of and subsequent to this paper, the Secretary of Defense directed some real concerted effort to relieve that situation. But top echelons of the executive must continually stay in contact with this facet or it will slip right back again.

We must become more conscientious in the declassification and the downgrading of classified information. This is really costing us and I believe we realize it. We should review our files every six months and the results have to go up to the Service Secretaries.

The last main conclusion — although scientists dislike secrecy, they generally recognize the necessity for certain security measures. They appear more sensitive about restricting basic research information. Restricting that kind of information bears the greater penality. The DoD policy that basic research projects at universities and colleges will be unclassified should be considered by all government agencies.

In summary, when you restrict R&D information, you are naturally going to impede the flow of information internally as well as to the enemy. You are going to have less informed private citizens, less informed government officials, and obviously it's going to cost you in manpower and equipment. That goes almost without saying. However, the requirement ultimately becomes a matter of benefits and penalties with the conflicting demands of democracy and national defense presenting a real dilemma. Determining an answer to the immediate question of whether security classification is bearable or intolerable must be based upon the needs of our entire country. It must also be recognized that in the long run when the proper balance between restriction and disclosure of scientific and technical information is not found, the price is going to be paid by every one of us.

* * * * *

SECRECY AND THE DISSEMINATION OF SCIENTIFIC AND TECHNOLOGICAL INFORMATION

BY

CAPTAIN ROBERT L. TAYLOR

The paper I am going to present to you represents a year long study that examined in depth the effects of Department of Defense security restrictions on the scientific and technical communication flow. Contributors to the study included persons in academia, industry, and government. Many of you participated and I would like to acknowledge specifically the assistance of Mr. Bob Donovan who patiently critiqued each of the many drafts.

The subject matter of my paper is closely aligned with the previous presentation with but two exceptions. First, I dealt more specifically with

Executive Order 10501. Second, the focus was on the flow of scientific and technological information. After historically reviewing the restrictions that exist today stemming from Executive Order 10501, I carefully examined the arguments for restrictions and contrasted them with the arguments against restrictions (such as those typified by Dr. Teller and other vociferous members of the scientific and technical community). However, I realize that there isn't an either or an or to this. It is instead, a continuum. Most of us find ourselves either to the right or to the left of center as to how we feel about restriction of scientific and technical information.

One of the most startling conclusions that I came to was that although the scientific and technical communities' objections are more publicized and found throughout the literature, they are in fact not substantiated with the same rigor and by the same rules that they require of their own scientific and technical research. There is very little empirical evidence that the advance of science and technology has been effectively impeded by restrictive actions as far as Executive Order 10501 is concerned. The argument of the scientific community appears to rest on (1) the Constitution, and (2) the free flow of information needed in the validation and verification processes of the "scientific method" (whatever that scientific method is). Why then do we hear only that one side?

We have heard logical, concise, and articulate arguments at this seminar supporting the intelligent use of security restrictions. Frankly, it does very little good to spread this gospel to two or three hundred people (including the Journal circulation) and have it go no further than that. We need cogent arguments to be presented in the scientific and technical literature. Publishing these arguments in the more formal media is one of the recommendations that I make in this paper.

Another conclusion is that too much effort has been spent on how we should administratively restrict information and how we should implement directives. Not enough emphasis is given to the dissemination of information. I would think that it would be a good workshop theme or even a seminar theme to concentrate on the activities of (1) getting information downgraded and declassified, and (2) disseminating classified information.

A third conclusion of the paper has received public notice because of recent events. That is the philosophy behind Executive Order 10501. Being over thirty and on the student side of academic life gives me a unique vantage point. The philosophy behind this Executive Order is probably respected by the majority of people in the United States today, but I doubt whether the same type of philosophy can be used in the next decade or two. Young people today demand more understanding and a deeper knowledge of the necessity for restricting information than "in the best interest of National Defense." We, in this Society, must take advantage of current events and make some strong recommendations — not with the present in mind but with an eye on the future — because these young people are going to be the ones in power in the next ten to twenty years. Their ideas are radical and different than ours. We must take this into consideration.

In an attempt to reconcile philosophical differences, I make another recommendation to separate classified military information from classified scientific and technical information, applying different rules to each. Computer technology, operations research, management science, and a number of other techniques can be used to handle administrative functions that cause the bulk of our day-to-day problems. Our attention must be turned toward generating ideas as to how we can disseminate scientific and technical information. This leads to the last point presented in the paper.

We need research that will identify the effects of security classification restrictions — research that is going to be accepted by those in the scientific and technical community. I am here not as a government classification specialist nor as an industry representative. My interest in this field is that of an academic investigator. I have tried to apply the methods of research to the fields of classification and classification management.

This paper is a descriptive study and as such, does not provide the type of evidence acceptable to a scientific or technical journal. However, I am now engaged in a quasi-experiment in a military in-house research and development laboratory where I hope to evaluate the technological gatekeeper phenomenon as it exists in all information flows compared with the phenomenon as it might exist for classified information.

Briefly, technological gatekeepers are individuals (professionals) within an R&D lab to whom colleagues turn for the most current information regarding a technical specialty or concerning a particular media. These people are called technical discussion "stars." These stars have been found to exhibit other external characteristics such as having a greater number of professional contacts outside the lab than their peers, they read more of the technical literature, they hold more patents, and they attend more professional meetings. The technological gatekeepers are defined by both the internal and external characteristics. The gate that they are keeping is the information flow external to the lab and they are channeling it to their colleagues within the lab. The management implications of this are tremendous. If you want to insure that your professionals have the most current information, you make sure that the gatekeepers get it.

In my current research project, I propose to evaluate the flow of classified scientific and technical information in the laboratory and compare it to the operation of this gatekeeper concept while controlling as many external variables as possible. Hopefully, the report of the results (combined with other such research) will get into the scientific and technical journals. At least this is an initial attempt at performing thorough and concise behavioral research in the area of classification.

Thus, I would make a strong recommendation that this Society sponsor a number of research projects. I am not talking about great sums of money; just your interest and enthusiasm along with your ability to help researchers by providing data and advice. At the same time, you have a great amount of resources available in the academic community like myself to undertake problems that you have. Perhaps we can come up with some answers.

The full text of this paper is contained in the June 1971 issue of Industrial Security. I invite you to read it and I hope that you do. If you have any comments or criticism, I would ask you to write. I would also ask you to take the recommendations into consideration and I hope that I can make some contribution to the theory and practice of classification management.

* * * * *

POSSIBLE APPLICATION OF DEPARTMENT OF DEFENSE VALUE ENGINEERING INCENTIVE PROGRAM TO CLASSIFICATION MANAGEMENT

BY

O. P. NORTON and T. C. CONNOR

[O. P. Norton's portion presented by Mr. Metz.]

[Mr. Metz] Someone once said if you were to ask employees how can we make more money instead of how can we save money, people would step forth with

many suggestions. And that observation is based on the concept that making money is loosening up and saving money is restrictive. Accordingly, the save money campaigns produce attitudes that cause people to hold back and on the other side, the idea of making money creates an attitude to encourage people to participate and to develop better ways to do the job.

This project which we are reporting on this morning is a good example of an idea of making money, because the Value Engineering Incentive Program is one of the government's programs to stimulate the contractors by offering to repay these efforts and increasing the contract price or fee, then the proposal must meet certain conditions in the contract proposal.

One of the basic conditions for proposal qualifying for acceptance under this program is to involve a cost reduction, and that cost reduction must involve a change in the contract.

Since changes in classification are provided in the security classification list which is a formal part of the contract, then the government's acceptance and action on the contractor's proposal would meet that basic requirement.

I'm not going to talk any more. I want to save the time for Tom who has a message that is more important — I think the engineering phase is more important than the security portion. I want only to say that we agree with Mr. Van Cook's recommendation in the workshop yesterday that a joint team basis be set up by NCMS to establish data or a firm cost that we can use in submitting this type of proposal.

[Mr. Connor] Yes, we agree with the Colonel that the gobbledegook and all the various conflicting laws, etc., are prime candidates for change, and what we were involved in at LTV was a method or a vehicle by which one could make money while doing it.

Mr. Norton came to me and proposed that we try to declassify some of our particular portions on the Lance Missile just coming into production as an Army weapons system. Mr. Norton also suggested that we should attempt to use Value Engineering Incentive Clauses which we had on our specific production item, and this is something you folks ought to think about in your own operation. I'm sure you have value clauses in your contracts.

I find that the older managers, whenever you're talking hardware changes or any type of method you want to switch around, have a deathly pall come over their features, but when you mention software revisions, they just don't seem to care. It seems to be an easier sell to change the latter.

What we were involved in was a particular portion of a guidance system. We felt that at the time the R&D program portion was over, there were items coming out of France using the same types of methods, and we felt that this was a good candidate for downgrading of security classification. What we were proposing was to downgrade this particular item, and in so doing, ran into a problem of how to calculate the dollar value involved. As a result, we had major difficulties in this area. We have since gone to various companies — Lockheed, etc. — and obtained their information on how they actually cost their documents out.

What we now have to have is some method of making the cost analysis that the government will buy. I have been involved in many engineering operations, and the auditors come about at the program end and really work you over to find out how you arrived at your numbers.

So, this is one of our problems. But as Mr. Norton indicated in his paper and in our joint paper, we feel that the NCMS should undertake and I understand there has been a Committee

appointed by NCMS to try to see if they can price out what classified documents would actually cost.

We have just been awarded something like $340,000 on a VECP item we submitted, not necessarily on classification. It was on a hardware change and we have made this and some additional money on the Value Engineering Incentive Program. I have a bibliography in the back of the paper which you can inspect at your leisure. There are some booklets in there that are relatively inexpensive. From them you can get a quick and real close example of what value engineering is all about. You can ask your contracts people, whoever you work with for additional information. I think that this is a method of making additional profit dollars and I believe that the government will benefit and so will your company.

Bibliography —

1. Department of Defense. Principles and Applications of Value Engineering. Volume I. Washington, D.C.: Government Printing Office — $2.00 each.

2. Department of Defense. Value Engineering. Handbook 5010.8-H Office of the Assistant Secretary of Defense. Washington, D.C.: Government Printing Office (12 September 1968) — $1.00 each.

3. "Technical Proceedings and Special Report of the 3rd Annual Technical Symposium," American Ordnance Association Technical Report. Washington, D.C., October, 1969 — $10.00 each.

4. "Profitable Value Engineering Through VECP'S," American Ordnance Association. Washington, D.C., October, 1970 — $8.00 each.

5. "Digest of ASPR -- Value Engineering Provisions," Society of American Value Engineers. Twin Cities Chapter, Minneapolis, Minnesota, July, 1967.

* * * * *

CLASSIFICATION MANAGEMENT TRAINING AND OPERATIONS

BY

JACK ROBINSON

Classification Management is a tool of Management; if classification management is to be good, the original classification must be good. As this is the heart of the program, a brief review of the status of classification authority and operations may be useful.

CLASSIFICATION AUTHORITY

The authority is, of course, inherent in the Constitution's provisions for the common defense. More practically, for our everyday use, it stems from Executive Order 10501, as amended, which says in part:

> Section 2. Limitation of Authority to Classify. The authority to classify defense information or material under this order shall be limited in the departments and agencies of the executive branch as hereinafter specified. . . .
>
> (c) In those departments and agencies not affected by the provisions of subsection (a) and (b), above, the authority for original classification of information or material under this order shall be exercised only by responsible officers or employees, who shall be specifically designated for this purpose. Heads of such departments and agencies shall limit the delegation of authority to classify as severely as is consistent with the orderly and expeditious transaction of government business. . . .

In consonance with the requirement

for delegation, each of the services has issued directives, specifying who may exercise original classification authority, and limiting it in relation to successively higher levels of classification.[1] There is no purpose in our repeating the detailed list of those who are so designated, but it may be useful to mention, in capsule form, the original authority for Top Secret classification. In each of the services and DoD these authorities are the Secretary and his principal assistants and staff, the Chairman of the JCS and his principal staff, and the Military Chiefs of Service and their deputies and heads of principal staff offices, and the Commanders of major operating forces and major field establishments. As specified, the authority may not be redelegated. In this connection, the phrasing of delegation in the Navy appears more extensive than in either of the other services; the Army appears most limited.

On the basis of numbers of people authorized to exercise original authority for Top Secret classification, the Air Force is the most liberal of the services. This is an essentially current list for the respective services and DoD:

TABLE I[2]

NUMBERS OF POSITIONS AUTHORIZED TO CLASSIFY TOP SECRET

OSD	20
JCS	40
Defense Agencies	226
Dept of Army	79
Dept of Navy	198
Dept of Air Force	240
Total	803

The total numbers of people authorized to exercise original classifying authority at the other classification level are:

Secret	7,687
Confidential	31,048

Derivative classification, about which more will be said later, stems from the further use of material that has been classified by an original authority. A person who uses such material in other ways or in other documents is exercising derivative authority. Such authority includes, of course, the use of guides in different fields announcing determinations made by higher authorities.

Mention must be made of the level next higher than the Secretary of Defense, namely, the Office of the President — specifically with respect to the National Security Council. The issuances of this office have a determining effect on classification when they enter the DoD in one way or another.

This, then, is the framework within which classification is created; there is ample opportunity for variations of interpretation, as one might suspect.

Classification is changed in a manner that parallels its creation; namely, any authority authorized to create can reduce or eliminate, and any authority in a higher chain can take such action with respect to issuances from subordinate offices. Of course, this requires thought, consideration, and deliberate action — all at a premium in a busy environment. To help, the Automatic, Time-Phased, Downgrading and Declassification Program was, as we all know, created;[3] it is in use by the services and their agencies and contractors. The program has been of major importance in keeping the amount of classified material within reasonable bounds. There are difficulties in its operation; I shall refer to them later. Some have been discussed at this meeting.

Another medium that has begun more recently to have an effect on changes, in addition to its effect on classification, is the classification guide, now operating as part of the Classification Management Program. A brief

---

Footnotes appear at the end of the text.

summary of the effect of the Classification Management Program on the issuance of such guides may be inferred from Table II.

TABLE II[4]

CLASSIFICATION GUIDES

Dept	No. of Guides 30 Jun 1963	30 Jun 1964	January 1971
Navy	17	22	130
Air Force	116	153	270

As we can see, there has been a steady improvement in the availability of guides — and, in general, their quality as well.

WHAT'S CLASSIFIED — Some Comments

Having determined who is authorized to classify and change or declassify, we now approach the question of what to classify. To rephrase the opening statement, good Classification Management depends on good classification.

Many comments have been made about the process of classification and the selection of material to classify. The basis, of course, is in EO 10501, which establishes the degrees of classification. About Top Secret, for instance, the document says:

> . . . The Top Secret classification shall be applied only to that information or material the defense aspect of which is paramount and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation such as leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.

As we know, the specifications for other categories are distinguished by changes in the value words concerning the potential effects of compromise. The problem is to determine whether compromise or loss could cause "exceptionally grave," or "serious," (Secret), damage or be "prejudicial" to the defense interests of the nation (Confidential); this problem faces all who serve as original classifying authorities or prepare classification guides.

To help in interpretation, DoD has issued Writing and Applying Classification Guidance,[5] and some of the service components have issued similar instructions, based upon the original, amplifying to fit their circumstances. In this area, a few additional words may be of some value. In assessments leading to a determination of classification, the potential of a given friend or possible foe can be based on a few relatively easy-to-discover facts, since information about raw materials, people, and other basic resources is generally available. The capability of a nation, based on its potential, becomes a more sophisticated element of information; some aspects are determinable with relative ease (e.g., the amount of arable land required to support given population under normal circumstances), other aspects only with great difficulty, if at all. In these days of advanced technology, a nation depends heavily on an industrial base that can regularly turn out uniform products of complex design. Assessing the extent and quality of the industrial base becomes a vast puzzle, pieces of which come to hand from time to time, and lead to such judgments as "the Soviet Union is approximately 5 years behind the U.S. in computer technology." The task of arriving at this judgment is essentially one of scientific and technical intelligence. The results may be classified or unclassified (as in the computer assessment), but evaluations of their application in military fields and comparisons of capabilities are generally classified.

Let us turn to the most difficult-to-determine aspect of information. Having established the capabilities or the range of capabilities, we must now consider intent. There is little question that if we can establish the intentions of a possible adversary, we have gained much. We may have been able to establish that a capability to do so-and-so exists, but the pinch is in deciding whether there is an intention to do it. The most obvious encounter with intent is in plans: war plans, contingency plans, development plans, etc.

As an illustration, the commander of a force in the field can develop a fairly accurate picture of the force he faces. Intelligence may establish that the enemy has troops and aircraft, so positioned as to be capable of reinforcing other forces within a stated time; knowing whether they actually intend to employ the force in such a manner can make a significant difference to the commander when he assesses the likely outcome of his plans.

It is interesting to note that of eight considerations to assist in initial classification determinations found in DoD 5120.34H,[6] four may be said to address themselves to intentions, three to capabilities, and one to time. Intent, therefore, is most critical; it must be assessed carefully. Concealing intent is particularly difficult in a country such as the United States; for one valid reason, the President may decide to reveal intent in order to further national policy. For another, intent must be related to capability; there is intense coverage of the area of capabilities in a plethora of trade magazines and papers. The difficulty and importance of evaluating intent and its relation to capabilities is emphasized a number of times in a supplemental statement to the Report of the Blue Ribbon Defense Panel, which said, at one point:

> It is imprudent, indeed even reckless, to formulate such policies [national defense policies] on the basis of subjective judgments as to Soviet and Red Chinese intentions rather than their known military and technological capabilities.[7]

Consequently, whether intent is revealed in information must be weighed and probably will be classified unless the classifier has positive knowledge that higher authority has authorized disclosure or release.

WHO CLASSIFIES — 2 basic approaches

Having discussed some aspects of what's classified, let us return to the question of who does the classifying. We have discussed the officials who are authorized to create classification in the first instance and have noted the part played by derivative classification. The framework seems reasonably clear-cut and straightforward. Surely, the effort should advance with little difficulty. Should there be problems?

The Author — A primary means of establishing classification — probably the most common — is to have the author decide. It is also probable that the author is not an original classifying authority. He may or may not be authorized to issue the paper he creates in his own name or in the name of his superior (who may be an original classifying authority). If the author does not literally sign the paper, but an original classifying authority does, that official is presumably exercising his classification prerogatives and confirming the classification, as is required of him by existing directives. Since hundreds of thousands of pages are created each year, it appears only reasonable that the author would have primary responsibility in establishing the classification: he should be best informed on the topic, and the wheels must keep turning. If, however, he does sign and is not an original classifying authority, on what basis does he establish the classification? Derivative authority? Issued guides (a form of derivative authority)? Personal expertise? Following the

prescribed path of finding an original authority?

Derivative classification is the most eligible peg on which to hang classification. In this respect, two basic problems have adverse effects on good classification. The first is an assessment of whether information drawn from an existing classified paper is classified. A foundation for derivative classification can be inferred from Section 3 of EO 10501 subparagraphs (a) and (b), primarily; these state in part:

> (a) . . . Documents shall be classified according to their own content and not necessarily according to their relationship to other documents . . .
>
> (b) . . . Documents separated from the file or group shall be handled in accordance with their individual defense classification.

In implementation of the concept, one finds for DoD:

> 1. Derivative classification is involved when
>
> a. An item of information or collection . . . is the same as . . . other information with respect to which there is an outstanding proper classification determination . . .; or,
>
> The information is created as a result of . . . other information . . . which has been and still is properly classified; or . . .
>
> 2. c. In connection with all operations where derivative classification of a document . . . occurs, definite procedures shall be established by appropriate authority so that, . . . the necessity, currency and accuracy of each derivative classification will be reviewed . . .

Note the emphasis on "proper," "current," and "accurate." However, in the next paragraph we find:

> 3. In those situations involving the copying or extracting of classified information . . . the individual . . . shall be responsible for assuring that the new document or copy bears the same classification as that assigned to the information . . . from which . . . prepared . . .[8]

The Navy, in issuing the above instructions[9] added to paragraph 3:

> 3. . . . copying or extracting of classified information clearly identified . . . [emphasis supplied]

Neither the Army nor the Air Force directly included that paragraph in their versions[10] but all services included the substance of the definition of derivative classification.

There is an additional aspect, one that often escapes recognition in the area of exercising derivative classification; namely, when does derivative classification end and original classification begin? As stated above, EO 10501 implies a foundation but does not cover "derivation" classification directly. In addition to Section 3, quoted above, related material appears in Section 4.b.:

> (b) Non-Automatic Changes . . . The downgrading or declassification of extracts from or paraphrases of classified documents shall also require the consent of the appropriate classifying authority unless the agency making such extracts knows positively that they warrant a classification lower than that of the document from which extracted, or that they are not classified.

The basis DoD instruction[11] in defining original classification includes:

> b. An accumulation or aggregation of items of information, regardless of the classification . . . collectively requires a separate and distinct classification determination.

The Army in its directive,[12] says:

> d. Original classification . . . or a compilation of information requires a classification based on the sensitivity of the combined information . . .

The Navy in its version[13] included the DoD instruction verbatim; the Air Force[14] restates and adds:

> b. An accumulation or compilation of items of information, regardless of classification or lack thereof, requires a new or different degree of protection.
>
> c. A currently classified item of information requires a different degree of protection or the removal of such protection . . . and the action taken is not in response to classification guidance from a higher echelon.

The purpose of the extensive cross-referencing and citation above was to establish the complexity of the framework within which a decision must be made. It also leads to the second basic problem in use of derivative authority. The individual author, despite his competence in his field, may find it difficult to determine:

— Whether there are issued classification guides on the topic or combination; and, if not,

— Whether the information he is presenting reflects determinations on classification previously made by "competent authority" and still current; but, if so,

— Whether the information represents a combination, elements of which were previously classified by competent authority but the combination of which is new.

In essence, the likelihood that the army of individual authors can be adequately informed in this field is quite small. Further, under these circumstances and the press of time, there is little question that "original" classification at all levels is being performed regularly by those who are not explicitly authorized to do so.

Central Office — The second of the two basic approaches to classification is to have it done by a "central office," rather than by the author. Here, a "central office" does not necessarily visualize a large group; it does mean one that exercises the authority for classification and classification management and is not responsible for any other major functions (and not many minor one, either). A number of points concerning this concept undoubtedly come to the mind of each of you. The points against such a concept probably can be reduced to three:

— Nobody knows that much

— Papers would never get out

— It would be too expensive

Before examining the matter, we should confess that our Group decided to go this route. Therefore, the reader should be aware of some probable bias in the direction of this solution.

The difficulties that face an author can be easily recognized as being different from those of a centralized source of classification determination. At any given time there is an existing milieu only portions of which are changing. This is not to say that there are not many changes but rather that if one has a fix on the setting one can perceive and absorb such changes more easily.

Illustratively, until about 1969, the fact that the basis for general-purpose force planning as set forth in the Joint Strategic Objectives Plan (JSOP) — 2 major contingencies and 1 minor, to be met simultaneously — had been classified for many years. As an existing part of the picture, one knew, without looking it up, that any information revealing that this was the case would be classified. After the decision to make the information public, that part of the picture changed; now information that does nothing more than reveal the announced basis — currently, 1 major contingency and 1 minor — for general-force planning is unclassified and publicly released. In essence, such a "set" establishes a small alarm that activates if one encounters information that goes beyond the limit in some way.

Similarly, the announced 4-1/3 division troop strength in current support of NATO is an announced fact and part of a picture that does not change quickly — one would recognize with relative ease information that went beyond those limits.

Hence, the problem that faces the army of authors — of whether there is a "guide" — is much simpler for a squad of classification managers.

The next difficulty that faces an author is whether the information:

> . . . is in substance the same as or closely related to other information with respect to which there is an outstanding proper classification determination of which the derivative classifier has knowledge . . .[15]

Some key words here are "in substance," "proper classification," and "has knowledge." If the question is specifically technical and in the author's field, the judgment can probably be made effectively. I submit that few of the determinations fit so neatly.

As an example of the difficulty, one may cite the most recent "Posture Statement"[16] of the Secretary of Defense. Of the 258 pages in the Secret version, only 57 pages contain classified information. The remainder appear verbatim in the publicly released version. Even on the 57 pages, a major fraction of the text is the same as in the unclassified version (not necessarily true of some tables and figures), and only a few elements of information are changed; the Secret version (which is not paragraph- or page-classified) surely represents classification by one of the top-level original authorities, and much "substance" can be derived that appears to require a Secret classification based on a "proper classification" by an obviously authorized person. In this case, the "has knowledge" problem of the author can be assumed to be easily resolved, but the comparative knowledge may be a different question.

A related aspect of this problem for the individual author is the "proper" part of "proper classification." Proper in the context cited, must also mean authorized, since a classification can be considered proper only if it has been performed by someone granted the authority.

In Table I, we established that the number formally reported as authorized to make original determinations at the Secret level is 7,687. It might be difficult to learn whether the information at hand was originally classified by one of this number. In fact, the difficulty of finding out would essentially preclude trying to learn, except in the most important and pressing cases.

Concerning this part of the problem, the "central office" is in a much better situation than the individual author. The "in substance" portion is a part of the whole picture that has been constructed — as is the "has knowledge" portion — simply because of the need for a conscious effort to make certain that everything available has been collected. In the

case of "proper classification," too, the central office is in a better position to determine whether the substance of the information fits well with current guidance at a given level and who is likely to be authorized to issue guidance in the topical field under consideration. In this connection, it seems reasonable to say that the NCMS and the Classification Management program have provided a better network to obtain such information than has ever existed. It might, however, be almost as time-consuming for a central office to learn about any given one of the 7,687 persons/positions as for the individual author — but rarely would this be necessary.

The last of the problems facing the individual author who is exercising derivative authority, is that of assessing the line-crossing combination effects, namely, whether he is, in fact, making an "original" determination. An author is concerned mainly with the content of his paper. He can have only a secondary concern, at best, about the nuances of effects on classification and about whether he is making an original determination and has authority to do it. In fact, even the level of classification all too often comes off poorly for the same reason. Regrettably, one still encounters problem-creating classifications, such as a one-paragraph memo establishing as Secret the fact that a service Secretary wanted to be briefed on a particular day on the results of a study, the subject of which was unclassified; and a similarly brief piece issued by a military chief establishing as Top Secret the fact that a given well-known problem needed to be reexamined.

Having established some of the ways in which difficulties faced by the army of authors are greater than the same difficulties faced by a squad of classification managers, we look at the three points raised against the concept of central determination of classification.

The first — "nobody knows that much" — has been discussed indirectly in the discussion of the difficulties faced by an author. Stated more directly, there is at least room for argument that a small central group can know a great deal, because accumulating the information on which to base determinations results in a body of knowledge. More, it also leads to who has knowledge and the combination here is especially valuable. I am not suggesting, of course, that one person is likely to be, at the same time, a microwave specialist, a nuclear physicist, an acoustical expert, a naval strategist, a military tactician, and a chemical wizard, to mention a few. However, I am suggesting that the amount of knowledge necessary to cover security classification competently in a variety of fields can be acquired.

The second problem is really a question of timeliness. Given that a central office can accumulate the necessary information, how long would it take to push paper through the process of classification paragraph by paragraph? Here, as one would suspect, cases may differ; still, we can talk about some general figures.

Two of us provide classification management for our Group. The Group is relatively small, having approximately 350 staff members on the "paper creating" side. The Group, however, has a large paper output, and a large document collection to provide the necessary information base. Recently, as part of our overall program, we examined a block of the collection for currency of classification. Of approximately 3500 titles considered, we selected 357 items for examination. The selecting was based on knowledge of subjects for which changed guidance existed. We were able to change the classification of 209 of these 357 items; we also found that a number of others would be eligible for classification change at an earlier date than had been originally established. We did the job in a month. During the same time, we considered and established classifications for newly created material. At the time, the number of items produced each day was

only a little over 3, although the normal is about twice that figure. These new items, of course, took priority.

At our Group, items range in size from 1 page to several hundred; commonly they run between 12 and 30 pages. Other tasks not covered in the counting process include review of some incoming material for downgrading group determinations, advice to members of the staff on what information one can use at the unclassified level, auditing of selected accountability records, and study — about which we shall have more to say.

The last of the objections raised to centralized classification concerns cost. This area certainly is the spongiest; little can be said precisely or with unchallengeable figures. People constitute the main expense. To some extent, the discussion of timeliness has covered cost, because of the relation of output to people. What we have not covered in the time (and, therefore, cost) saved the authors, who can be assumed to be relatively high-cost people. Nor is there yet an agreed-upon set of figures for the amounts saved (or avoided) by reduction of the level of classification or the creation of a paper at a lower level of classification or unclassified. These questions do not, of course, even touch on the value to be accorded proper classification — the reason for the whole game.

There is an inherent advantage in the existence of a group of "central offices." In part, some advantage has already accrued as a result of the existence of this Society, some because of the classification management program. I hope that the trend will continue because in it there is potential for far better classification. It is well to remember that EO 10501, Section 4, establishes the requirement:

> . . . Heads of departments or agencies originating classified information or material shall designate persons to be responsible for continuing review of such classified information or material on a document-by-document, category, project, program, or other systematic basis, for the purpose of declassifying or downgrading whenever national defense considerations permit, . . .

This aspect, too, can be better served by a group of central offices, since, as we have seen, classification is a continuum, and continuity and interchange of information among such offices can promote a more effective program.

QUALITIES OF A CLASSIFICATION ANALYST

Assuming, for purposes of further discussion, that a central classification office is to exist, who should be in it and what training is necessary? It may be said that there is not just one set of criteria; rather, there is a spectrum of possibilities.

Background — There is little doubt that, since the frame of reference is national security and defense, a background in defense matters is very important. Service in one of the Armed Forces for some reasonable period of time, especially in positions that required an understanding of the employment of the force and its interrelationships with other armed forces, is very desirable. Lacking such experience, the person would, at the very least, have to have considerable interest in these matters. Certainly, even with experience, one is likely to have to learn a great deal. As well, the desirability of a background in technical or scientific work is clear. The particular field or fields (if one is so fortunate) is not specifically important, unless the information area to be covered is sharply circumscribed. If not actually experienced in matters technical and scientific, the person must at least have strong interests in the direction.

Interest is a critical factor and the emphasis is not misplaced. To return to the first objection postulated to

the concept of a central office (nobody knows that much) and to the discussion of the point, it is true that any person entering such an office will have to be oriented toward continued learning. It is true also that learning is not everybody's dish of tea. Care must be exercised to make the point quite clear.

Training — When one then enters into a "central office" type of organization, there is bound to be a period of training — mostly on-the-job or self-training. Naturally, the particular program for a given individual will be related directly to his particular background; thus, it is unlikely that two programs would be identical. Similarly, the particular organization is likely to have areas of emphasis; these provide a topical guide to the study effort. In any event, some general elements to be included can be stated:

— General handbooks on military operations of all services, with emphasis, as appropriate, on the principal service association — both classified and unclassified items.

— Documents and books concerned with the basic principles that underlie hardware development (e.g., Physics of Sound in the Sea,[17] and The Effects of Nuclear Weapons,[18] electromagnetic theory books and documents, etc.).

— Intelligence documents.

The study phase will probably take several months for a reasonable feeling of comfort in a small number of fields; actually, study is a continuing requirement. It should be interspersed with discussions, inside the classification management group on aspects related to classification, and with other members of the staff on technical aspects of the work.

Concurrently, the training should include examination of material both well classified and poorly classified. Beginning about the second month, and proceeding concurrently with study and the examination of examples of classified material, some practice on classification of new material should be undertaken. Such practice forms the base for applying information already gained and determining whether the study phase has covered the area adequately, as well as discussion and further guidance.

Subsequently, with experience and confidence, the trainee would actually classify material under the guidance of an experienced analyst. As training proceeds the emphasis should shift to having the trainee bring up points on which there is some uncertainty. After eight months to a year, the individual will probably be able to operate independently.

Continuing Operations — Some comments are necessary. Of prime importance is the necessity to recognize that a reasonable amount of time must be available for continuing review and study — perhaps a third of the total time — for both studying related material and seeking out new information. It may be thought that one may expect to acquire new information by requesting it on a continuing basis. Experience has shown, however, that the process is rarely foolproof.

An important source of both guidance and information about classification is to be found in Congressional hearings, principally (but not exclusively) related to the DoD. These should be studied for application in the determination of classification.

As mentioned earlier, another important source of information is official statements, especially the "Posture Statement" of the Secretary of Defense, to which I have referred previously, as well as other members of the DoD and the Services. Again, these have to be examined in detail, from the point of view of both what they include and what they omit.

Active steps must also be taken to study newly issued classification

guides. Guidance may have to be provided operating members of the organization. In a related area, documentary issuances of other organizations should be examined, for currency in various fields, both for the information content and for the classification applied.

Last, we should discuss matters with technical people from time to time — both for better understanding of the technical aspects of a problem (how does side-lobe detection compare with main-lobe detection) and for the aspects of information that are to be considered sensitive (what isn't known about OTH) and why.

SUMMARY

The purpose of this paper was to present an approach to classification management training and operations. It is surely not earth-shaking, revolutionary, or visionary. Of necessity, it has dealt far more extensively with "where it's at" than with details of how to select and train. However, in the view of the author, the "where it's at" and "how it is" is critical to approaching the goal of better classification management through better classification. As is evident to those in the field, the recommendations for central office determinations contain technical questions of propriety. These do not seem insoluble. More to the point, they are not technically worse than "how it is" now — and probably better. The paper is recommended to your further consideration.

Notes —

[1]DoD Instruction 5510.47, Safeguarding Classified Official Information, 2 June 1964. Department of the Army, AR 380-5, Safeguarding Defense Information, March 1969. Department of the Navy, OpNav Instruction 5510.1, Security Manual for Classified Information, 12 May 1969. Department of the Air Force, AFR 205-1, Safeguarding Classified Information, 2 January 1968.

[2]Information furnished by the Office of the Assistant Secretary of Defense (Administration) in May 1971.

[3]DoD Directive 5200.10, Downgrading and Declassification of Classified Defense Information, 26 July 1962. Implemented in the services by AR 380-6 (Army), OpNavInst 5500.40 (Navy), and AFR 205-2 (Air Force).

[4]Department of the Navy, NavPubInst 5215.41, Navy Directives System Consolidated Subject Index of Unclassified Instructions, of 30 June 1963 and 1964. Department of the Navy, NavPubInst 5215.51, Navy Directives System Consolidated Subject Index of Confidential Instructions, of 30 June 1963 and 1964. Department of the Navy, Office of the Chief of Naval Operations, Confidential Letter, Serial 010023P92, Subj: Index of Department of the Navy Security Classification Guides; forwarding of, 1 February 1971. Department of the Air Force, AFSC/AFLC, Security Classification Guide, of 1 July 1963 and 1964, and 1 January 1971. The figures in Table II are not exhaustive (e.g., DD 254s are not included). They represent the best comparative source however. A similar compilation for the Department of the Army was not available.

[5]Directorate for Security Policy, Office of the Assistant Secretary of Defense (Administration), DoD 5120.34-H, Writing and Applying Classification Guidance, 1 July 1968.

[6]Ibid., Chart 1, pp. 3-5.

[7]Supplemental Statement to Report of the Blue Ribbon Defense Panel, The Shifting Balance of Military Power, submitted to the President and the Secretary of Defense on 30 September 1970, pp. 2-3. Reprinted as Appendix 9, Naval Nuclear Propulsion Program-1971. Hearing before the Joint Committee on Atomic Energy, Congress of the United States, 92d, 1st Session, March 1971.

[8]DoD Inst 5510.47, op. cit., pp. 12-13.

[9]OpNavInst 5510.1, op. cit., pp. 4-9.

[10]AR 380-5 and AFR 205-1, op. cit.

[11]DoD Inst 5510.47, op. cit., p. 10.

[12]AR 380-5, op. cit., pp. 2-4.

[13]OpNavInst 5510.1, op. cit., pp. 4-7.

[14]AFR 205-1, op. cit., p. 22.

[15]DoD Inst 5510.47, op. cit., p. 12.

[16]Statement of the Secretary of Defense Melvin B. Laird on the Fiscal Year 1972-76 Defense Program and the 1972 Defense Budget, before the House Armed Services Committee, 9 March 1971.

[17]Summary Technical Report, National Defense Research Committee, Office of Scientific Research & Development, Division 6, Volume 8, Washington, D.C., 1946.

[18]Samuel Glasstone, Editor, published by the Atomic Energy Commission, Washington, D.C., 1962 (Rev. 1964).

* * * * *

POSITION PAPER ON RETENTION OF CLASSIFIED MATERIAL, PARAGRAPH 5, DEPARTMENT OF DEFENSE INDUSTRIAL SECURITY MANUAL (DoD 5220.22M) APRIL 1970 (Revised)
BY
NATIONAL CLASSIFICATION MANAGEMENT SOCIETY — NEW ENGLAND CHAPTER

Outline —

Section Title

Foreword —

The National Classification Management Society (NCMS) compiled this paper to express its position and philosophy concerning the disposition and retention of classified material by industry. The paper relates specifically to paragraphs 5ℓ and m of the Industrial Security Manual for Safeguarding Classified Information (ISM) (DoD 5220.22M) April 1970 as revised.

The NCMS position expressed here is based on the experience of industry and a judgment and evaluation of that experience. The effect of this proposal on the Department of Defense has been considered. No attempt has been made to relate the affect of the proposal on existing federal statutes, executive orders, and military regulations. The proposal may be accepted by modification of certain DoD regulations. Changes to existing laws or executive orders are not required.

The position expressed in this paper may result in an entirely new philosophy for the retention of classified material by industry. This philosophy will reduce the administrative workload created by current policy. There are provisions for the constant protection of classified defense materials in the possession of industry. The paper presents a radical departure from the present system together with the rationale and criteria for the change. Although some of the rationale could be used to modify existing procedures, the overall implementation of this proposal would be more logically and economically feasible.

Section I — Statement of Problem —

Current Department of Defense policy concerning the retention of classified material by defense contractors should be changed to conform with existing conditions in government and industry. The interpretation and implementation of the retention policy by government contracting agencies, military services, and defense contractors varies greatly due to their organizational

structures and philosophies. It furnishes adequate protection for classified defense information, but should be more concise in the protection of the proprietary interests of industry.

The problem is to establish a program for the retention of classified material by industry which will:

a. Insure the constant protection of classified defense information in the possession of industry.

b. Protect the proprietary interests of industry together with the defense posture of government.

c. Reduce routine and repetitious administrative workloads.

d. Eliminate confusion resulting from the interpretation and implementation of the retention policy.

Section II — Proposal —

The National Classification Management Society suggests that paragraph 5ℓ and m, DoD Industrial Security Manual, be changed to read:

5. GENERAL REQUIREMENTS

The contractor shall be responsible for safeguarding all classified information under his control. In the Furtherance of this Requirement, the Contractor — (subparagraph a-k follow)

1. Disposition of Classified Material: May retain, destroy, or return to the originator or source all SECRET and CONFIDENTIAL material received from authorized sources or generated/reproduced under the provisions of this manual. TOP SECRET material will be retained in the same manner as SECRET material unless otherwise directed by the contracting officer. Retention is predicted on the following conditions:

(1) The contractor is competent to perform on User Agency contract programs, and on independent research and development projects in the scientific and technical areas to which the classified material pertains.[1]

(2) The contractor maintains an adequate and satisfactory program for handling, storing, and accounting for classified material under the provisions of this manual as approved by the contractor's cognizant security office.

(3) Retention of classified material is dependent upon the contractor's ability to maintain an appropriate facility clearance under the provisions of this manual as approved by the contractor's cognizant security office.

Section III — Cognizant Security Office Responsibilities —

The cognizant security office referred to in the proposed paragraph 5 is the cognizant security office as defined in paragraph 4, Department of Defense Industrial Security Manual, April 1970. In cases where more than one cognizant security office is operating within a facility, responsibility for retention of classified material will rest with the office responsible for the security of the User Agency program.

Cognizant security offices shall be responsible for insuring that contractors meet the retention criteria for classified material as defined in the recommended paragraph 5ℓ, Department of Defense Security Manual. This assignment of new responsibility and duties to the cognizant security office should not require changes in

---

[1] When retention of classified material cannot be justified under the provisions of paragraph 5ℓ(1), the contractor may request retention authority through the cognizant security office to the User Agency representative concerned.

manpower or operating procedures. The basic requirements of our proposed retention system merely require a slight shift in emphasis in the cognizant security offices' existing duties. Cognizant security offices are currently charged with the responsibility for monitoring the contractors' programs for handling, storing, and accounting for classified material. To this end, they are assuring compliance with the Automatic Time-Phased Downgrading and Declassified System; examining the contractors' libraries, document storage vaults, and similar areas where there may be a potential for stockpiling or hoarding documents; and verifying that the contractor has an adequate, effective system for destruction of classified material.

The review of a contractor's competence to retain residual classified material (paragraph 5ℓ (1) should consist of a review of the contractor's list of current contracts which is furnished in accordance with paragraph 5z, DoD ISM. Contractors normally maintain records of closed contracts together with those records required by the ASPR and such fiscal and legal records as may be required by federal and state laws. These records will also indicate competence based on past performances.

Cognizant security offices may instruct the contractor to make available his field of interest registers. In addition the cognizant security office may request, when a need is indicated, additional proof of competence as outlined in section three of this paper. It is recommended that the contractor's areas of competence be established within one year of the implementation of the proposed retention procedure. The areas of competence should be reviewed annually or when extenuating circumstances indicate that there is a need for review.

Cognizant security offices are currently responsible for insuring that the contractor maintains continued eligibility for an appropriate facility security clearance. The ISR/ISM provides for a review of the facility security clearance to protect against financial instability, changes in ownership, foreign interests and continuing needs. To this end the contractor should not be allowed to maintain a facility clearance or a specific level of facility clearance solely for the purpose of retaining classified documents.

The recommended policy for the retention of residual classified material relieves PCOs and ACOs of their duties pertaining to the retention of classified material. However, this does not relieve any User Agency of the responsibility for protecting and safeguarding its classified information in compliance with paragraph 4 DoD ISM. A PCO, upon completion or termination of a User Agency contract will prepare a final Contract Security Classification Specification, DD Form 254, indicating current classifications, custody of the classified material, or the transfer of the classified material to a current contract. Upon receipt of the final DD Form 254, the cognizant security office will assume responsibility for the residual material as specified in the recommended retention program. The PCO will then be relieved of responsibility for the residual material. The cognizant security office must maintain copies of final DD Form 254s for each of the contractor's closed contracts. However, this action is being accomplished today whenever the contract is granted permission to retain residual documents.

Section IV — Area of Competence —

Prior to further analysis of the proposed change, the terminology of "contractor competence" is defined as follows and will be referred to hereinafter as "Area of Competence" or "Competence."

The proposed retention requirement for residual classified documents states:

5.ℓ (1) The contractor is competent to perform on User Agency contract programs, and on independent research and development projects in the scientific and technical areas to which the classified material pertains.

The contractor's competence within the meaning of the proposed requirement is defined as those scientific and technical fields in which the contractor may reasonably be expected to perform in a satisfactory manner on a User Agency contract.

Performance on current User Agency contracts is indicative of competence. Past performance on User Agency contracts will indicate competence. The establishment of fields of interest by use of capability brochures, independent work and/or other contract activities with DoD or other Government agencies will support the contractor's claim to an area of competence.

When there is an indication that current and past contracts together with the field of interest registers do not support the contractor's claim of an area of competence, a review of the technical qualifications of the management and engineering personnel of the contractor may be used to establish competence to perform in a specific area. The action normally will not be required for major contractors. However, in small facilities, universities, study and research corporations, etc., this review may be a guide to competence.

A review of the contractor's patents and patent applications will indicate an area of competence. The contractor may also use his proprietary information to prove independent research within a given area.

It will be the responsibility of the contractor's cognizant security office to authenticate the contractor's areas of competence. Contractors must currently furnish cognizant security offices with information pertaining to open contracts. Contractors should have available for inspection by the cognizant security office, their field of interest and capability data on requests. It will be the responsibility of the contractor to prove his areas of competence on a request rather than a recurring basis.

When a contractor is unable to establish areas of competence within the meaning of the above description, he may request authority to retain documents from the Chief of the User Agency concerned through his cognizant security office.

Section V — Functional Analysis --

A — EFFECT OF EXISTING AND PROPOSED POLICIES

When establishing a defense contractor, the government requires a contractor to sign an agreement (DD Form 441) to apply to established regulations in the ISM. The ISM is the only uniform regulation authorized for application in safeguarding classified information while it is in the hands of defense contractors.

While all contracting organizations in the DoD and the military apply the ISM to industry, each of these organizations has their own regulations and instructions to augment basic policy documents relating to security classification and contract matters. A similar condition exists in industry. All defense industries agree to abide by a uniform regulation, the DoD ISM. However, each industry has its own unique organizational concept and structure just as each military service or government contracting agency is uniquely organized. The existence of this condition may be the largest contributing factor to the problems of the retention authorization policy.

An extensive review of the development and growth of the policies and rationale concerning the retention of classified material by defense contractors indicates that the current policy is not suitable for present conditions

and needs. This rationale has become obsolete with:

a. The growth and development of competent cognizant security offices

b. The increase of technological competence of the contractors

c. The implementation of effective classification management programs within government and industry.

One overwhelming fact established by this review is that industry is left in a much less flexible and disadvantageous position in the overall matter of retention, control and responsibility for safeguarding classified material. A very important fact magnified by the review was that there is no traditional or uniform pattern for disposition or retention of classified material regardless of the specific ISM provision relating to this subject. Present policy has resulted in neither an equitable nor a significant reduction in the amount of classified information held by industry. This condition results from the extreme variances in the interpretation and implementation of the policy by large numbers of individuals with all degrees of background and training.

Cognizant security offices today are competent to judge a contractor's continuing capability to handle, process, and retain classified defense information. The volume of classified material in the hands of contractors is more readily controlled by effective downgrading and destruction programs and by costs than it is by retention regulations. Therefore, it is concluded that paragraphs 5 ℓ and m, DoD ISM place an unnecessary administrative burden on contractors and user agencies which is avoidable. The automatic retention of classified defense information by contractors together with the effective control and inspection by competent cognizant security offices will:

a. Reduce administrative work loads

b. Provide for a more equitable and reasonable dissemination of classified technical information and data within government and industry

c. Will insure a maximum security protection for classified defense information in the hands of industry

d. Will reduce the total volume of classified defense documents in the hands of industry.

The following specific subjects and functions chosen for this analysis are the major problem areas for industry. We believe this analysis and discussion will be helpful in recognizing current needs. It will also provide a balanced view of the effect of the proposed change on government and industry.

B — NO BID REQUESTS FOR PROPOSALS AND QUOTATIONS (RFQ)

Present policy requires the return of all material received with a request for quotation upon which the contractor chooses not to bid. Paragraph 5, DoD ISM makes no provisions for the retention of this material. However, the retention of this information will be of benefit to both the government and the contractor. Contractors determine current and future government requirements through normal marketing and procurement channels and through technical objective documents during technical briefings, etc. Requests for quotations are frequently a summary of this information directed towards a specific need. A study of the information received with the RFQ together with other marketing and procurement information will allow the contractor to determine current government needs and future requirements. These studies frequently result in contractor funded programs for product improvement and development. The results of these programs will be presented in unsolicited

proposals or in response to other RFQs.

On occasion a contractor is unable to respond to an RFQ due to prior work commitments or temporary shortages of competent technical manpower. The contractor may desire to bid on future programs for related of similar projects. Retention of RFQ information would allow the contractor to establish technical and management teams to organize future work resulting in a comprehensive, and cost effective proposal.

Often the contractor does not desire to respond to the prime RFQ, but he may be interested in becoming a subcontractor. The retention of the prime RFQ would benefit all concerned because of its more explicit and detailed information. The same situation is also applicable when the User Agency initially prepares an RFQ for a total weapons system, and subsequently cancels the RFQ, and prepares new RFQs for major components of the system.

C — PROPOSALS, SOLICITED AND UNSOLICITED

Under the current policy, a bidder or proposer is obligated to pursue the formal channels for official and legal authorization to possess material that is unique to his capabilities and area of competence. When proposals require research and development, study, product improvement, state of the art changes, technological advances, etc., the contractor includes his best technical approach and solution to the problem. After initial proposals are submitted, User Agencies often request additional technical information resulting in solutions to problems which are on the edge of, or are beyond, current technology. Proposals contain program management and organizational plans supported with cost analysis which is invaluable for future work. Many proposals, particularly those which are unsolicited, are based on company funded programs and contain technologies which are too far advanced for current government needs, but which will be usable in the future. It is vital for the contractor to retain this material in order to establish his proprietary and patentable rights.

The marketing, study, analysis, research and development, procurement and production cycles are so complex and interrelated that the combined proposal and bid data represent only a fraction of the total work effort expended in a response from industry. Much classified defense information is received or generated and subsequently utilized in proposals which cannot be readily identified with a specific procurement effort.

D — RESIDUAL CONFIDENTIAL MATERIAL

It is impossible to account for residual classified information as specified in paragraph 5m(4) DoD ISM if the contractor complies with the accounting procedures for CONFIDENTIAL material which are established in paragraphs 12, 17, 18, and 19 of the ISM. Logs, registers, and similar accountability records for CONFIDENTIAL material do not have to be reconciled or balanced. Continuous receipt systems are not required. Reproduction requests and records are not required. The destruction of CONFIDENTIAL material requires no written records. Estimates of CONFIDENTIAL material by type, subject matter, and approximate number, as required by paragraph 5m(4) are impractical for any but the smallest contractors. Estimates of this nature made with any reasonable degree of accuracy would require an excessive administrative work load. Notwithstanding the provisions of the ISM, contracting officers frequently request specific lists of documents, certificates of destruction, or specific document identification, all of which are not available through current accounting systems for CONFIDENTIAL material.

E — PCO/ACO FUNCTIONS

By directives, the PCOs are responsible for furnishing security guidance and other instructions required to

insure the safeguarding of defense information. They presently retain this responsibility until all classified information is returned to government control. Therefore, it is in the best interest of the PCO to recover all classified information furnished for a User Agency contract, program, or project to terminate their security responsibilities and thus concentrate on other active programs and administrative functions. The ACO duties are normally limited to obtaining security clearances for contracts and administratively processing requests for the retention of residual classified material. As the PCOs and ACOs normally operate under the regulations set forth by their military services, they tend to use these regulations as precedence over the provisions and intent of the ISM. Classified retention requirements of the ISM tend to be overlooked as a contractual accountability requirement in the same manner as other government-furnished equipment. The PCOs and ACOs are seldom in a position to realistically evaluate the retention requests of the contractor. Current User Agency policies vary from formal limited and conditional permission to retain, to automatic denial of retention requests with no logical basis for the variants.

It is not the purpose of the proposed retention regulation to remove the control of classified defense information from government agencies. It is our recommendation to shift the responsibility for residual classified information from the PCO to the Cognizant Security Office. The prime contracting officer will remain responsible for the initial dissemination of classified information and for the preparation and issuance of adequate and current security guidance. Upon completion of a contract, the PCO will prepare final security instructions for the contractor. For this purpose, a contract will be considered complete when all deliverable items under the contract have been accepted by the User Agency. Normally the final security instructions will be a Contract Security Classification Specification, DD Form 254, with supplemental data and instructions. The DD Form 254 should indicate that it applies to the material being retained by a contractor, or that accountability for the residual material is transferred to another contract or program. The DD Form 254 should also indicate that the facility's cognizant security office will now assume the responsibility for insuring that the contractor continues to safeguard the classified material under the proposed retention program. When this is accomplished, a security clearance for the contract concerned may be issued and the PCO may retire his files from a security point of view. From this point forward, requests from the contractor for additional or revised security guidance will be forwarded to User Agencies concerned through the facility's cognizant security office. These requests may also be forwarded to the Department of Defense Classification Review Board.

F — THE RELATIONSHIP OF CLASSIFIED INFORMATION TO SPECIFIC CONTRACTS

It is not possible to directly relate all classified material in the possession of a contractor to a specific government contract. This fact is recognized in the Industrial Security Manual, paragraph 5a, footnote 5, and paragraph 11.

As a result of establishing field of interest registers or their equivalent, contractors receive many classified documents from government agencies which relate to multiple contracts or subjects. To account for and dispose of these documents for each contract concerned involves unnecessary work and duplication of effort.

Contractors are involved in research and development projects which involve the extraction or compilation of classified information from many sources. They also frequently generate documents such as brochures,

presentations, unsolicited proposals, and technical planning documents which contain information derived from many contracts. Marketing activities by the contractor and program reviews requested by User Agencies frequently result in the generation of documents. These documents cannot be directly related to a specific contract. Qualified contractor personnel frequently attend meetings, seminars, briefings, technical discussions, etc., where they are exposed to classified information which is not directly related to current contracts. The subsequent analysis of this information frequently leads to the development of new ideas in technologies for which there is no classification guidance and which cannot be specifically identified as derivative in nature.

Patent applications, patents, and proprietary information often contain classified information not related to specific contracts. In this area there may be some question as to the contractor's right to assign a classification to the information and/or the government's right to insist upon a classification. Contractors will normally classify on the basis of derivative information and/or their knowledge in the government's involvement in the technical area concerned. In other cases, government agencies will assign classifications to contractors' patents or proprietary information because they consider it to be in the best interest of the national defense.

G — PRIME — SUBCONTRACTOR RETENTION ACTIVITIES

The retention of residual classified material by subcontractors involves all of the problems which concern prime contractor. The subcontractor must direct his request for retention to the prime contractor. As the prime contractor is not authorized to grant a subcontractor permission to retain residual material, he must forward the request to the PCO. PCOs are frequently unaware of the needs or requirements of subcontractors. Consequently, they rely heavily on the recommendation of the prime contractor. Subcontracts are normally completed prior to prime contracts. Therefore, add-on or follow-on contracts have not been awarded, and it is difficult to justify the retention of the subcontractor's material. At times a subcontractor may become a prime contractor for additional procurements. In this case, as in the case of RFQs and proposals, the subcontractor may be submitting his request through an unsuccessful and sometimes competitive bidder who will not favorably consider his request.

H — VOLUME CONTROL OF CLASSIFIED DEFENSE INFORMATION

The proposed retention program will not result in stockpiling of classified documents to any greater extent than the present provisions of the DoD ISM. The existing administrative options available for the User Agencies for authorizing the retention of classified information by contractors have the potential for causing the stockpiling of classified documents. The retention of classified material by contractor is a negotiable item with the User Agency. Consequently, there is no incentive for the contractor to establish uniform retention policies. Contractors presently attempt to obtain information from as many sources as possible in the hopes that they may retain at least a portion of this material. The result is frequently a massive duplication of information.

In most cases Security costs involving classified documents are included in a contractor's overhead or administrative charges. They cannot be applied directly to a specific contract. The proposed retention program would allow a contractor to establish permanent technical reference libraries and files. This, then, would be an incentive for the establishment of records management programs which in turn can be used to reduce the contractor's overhead costs through effective budget control.

The maximum application of the Automatic Time-Phased Downgrading and Declassification System (ATDDS) will serve as an effective means for reducing the volume of classified material on hand. Current proposals for the modification of ATDDS would further reduce the amount of classified information in the hands of a contractor. Cognizant security offices must stress and insist upon constant and immediate application of the ATDDS.

The stockpiling of classified information, poor accountability and control procedures, and lax or ineffective destruction procedures are all interrelated. Cognizant security offices must maintain a close check of Document Control systems, central filing procedures for classified information, accountability records, and destruction procedures and records. The contractor then has additional incentive to destroy surplus and unnecessary material.

I — THE EFFECTS OF AUTOMATIC RETENTION OF COMPETITIVE BIDDING

The automatic retention of classified material by contractors should not result in unfair competitive bidding between large and small contractors. The recommended proposal allows each contractor to retain classified information only within his area(s) of competence. Although a major contractor may have a large amount of classified information, the proportionate amount of information per area of competence should not exceed that of the small contractor.

All industries currently have access by official authorization to government repositories based on their current capabilities in direct relationship to their current contracts and fields of interest. The qualifications for receiving government repository information is the same for smaller industries as it is for the major industries. If the proposed retention authorization applies equally to prime and sub or associate contractors, there should not be a bidding advantage for any particular industry. Automatic retention of classified information will greatly reduce the number of requests for material from government repositories. This will result in a cost savings to both government and industry. It should be a much greater advantage to the small industry which has less time to devote to the collection of technical reference material.

Section VI — Conclusion —

Based on the foregoing analysis and discussion of factors concerning the proposed change, we believe this proposal, if adopted, would have the following effect.

a. General

1. Create a workable uniform and consistent national policy that can be employed by the government and industry with minimum time and cost for application.

2. Update a national policy within existing capacity and means to control and monitor classified defense information.

3. Help develop lead time and induce studies promoting and enhancing a proposing initiative in the technological areas of research generally assigned to the defense industry scientific community.

4. Give defense contractors the chance, within their areas of competence, to keep abreast of changing technology and help stimulate research efforts not so much at the initial expense of either government or industry.

b. Specific

1. Shift the responsibility of classified material retention and follow-on monitoring to the cognizant security office after the PCO has issued the final Contract Security Requirements (DD 254).

2. The PCO would retain the responsibility of disseminating the initial and final Contract Security Requirements.

3. Relieve the User Agency's representative of recall responsibility.

4. Allow industry to maintain at hand its own inputs and apply them to future bids, proposals or current programs.

5. Give bidder/proposer the option, at no cost to the government to retain, destroy or return any information in these categories.

6. Eliminate the problem of relating RFQ and proposal input data to a specific current or future contract.

7. Eliminate problems for the User Agency and contractors regarding subject matter and approximate quantity of unaccountable Confidential material.

8. Eliminate the costly time consuming chain of three or four phases of communication and correspondence among subcontractors, prime contractors, User Agencies and cognizant security offices presently required for authorization to retain classified material.

9. Allow the subcontractors and prime contractors to communicate directly with their cognizant security offices on matters regarding retention.

10. Require better and more extensive application of the automatic downgrading/declassification system.

11. Require the cognizant security offices to put more emphasis on retention, destruction, technical libraries and monitoring of contractor systems.

12. Allow industry more options for technical library systems and reduce cost to the government by decentralization of classified technical libraries.

13. Induce contractors to develop better systems for controlling classified information in their possession.

* * * * *

SPECIAL SESSION, JULY 15, 1971

The Chairman, Mr. Satterfield: There has been a slight change in the proposed program.

You know, as a result of the current news concerning classification management in national defense, the Society has fallen into a situation whereby we anticipated that we had a unique opportunity, and we do have a unique opportunity, to make some great strides in the near future.

All of you heard Don Woodbridge at luncheon — his quite impressive presentation — and I'm sure that some of the people were even somewhat emotional. In communicating with him earlier concerning our program, Don gave me a few words which I will quote: "Surely we have moved out of a humdrum and into an exciting situation. The Pentagon Papers are a crucial event in the classification management enterprise."

Now, during the week we have been somewhat rigid in our control as far as the topics that would be discussed during the seminar. We had a preplanned program, a theme — namely, Research and Development; that is, managing security in the research and development type environment. The program was planned months ago. All speakers were set up to make their presentations. Maybe for the good of the Society, and I think very much so for the good of the Society, we debated what should we do.

We have set aside — or we did set aside time to discuss what we might say of the Pentagon Papers. It was totally unrehearsed. We had one volunteer as Moderator for this particular session.

But unbeknowing to any of the Board of Directors (we were at luncheon), we came in and faced the lights. The Board of Directors were called together and a decision, somewhat, was made in the debate as to whether we should continue under these circumstances.

There is somewhat of a feeling that even though many of you have personal feelings towards what has happened — I'm sure that many of you would have had lots of information, in your personal position, lots of information to pass out. But the Board is of the opinion that due to the, we might say, pressures and the reflection maybe on the company or the government agency or the location, the individual himself might be reluctant to really and truly participate.

In addition, the Moderator, of course, was quite concerned, but an individual quite capable of handling any situation whether there was TV coverage or not. But still as a result of the information that has appeared in news, as an individual, he decided that he preferred not to moderate the open forum.

So, it appears to me that about the only thing we can do is move into the part of the program which was earlier scheduled, in fact, the way that our program presently appears.

Comment from the TV Camera Crew Manager: Sir, excuse me. I don't want to interrupt your meeting, sir, but I think there's been a misunderstanding. We did not know this was a closed meeting. Since it is, we'll take down our cameras and go. It's just a misunderstanding. We don't want you to change your program because of television. We had been, or through some mix-up had been — were here to hear a speech by a man named William Florence. And if that's a mix-up, we'll take down our equipment, if you'll give us ten minutes, and be gone. I'm very sorry.

Mr. Satterfield: Well, a decision was made, I guess basically. We're in a situation whereby . . .

TV Crew Manager: I regret this misunderstanding.

Mr. Satterfield: It would take time for you to take down your equipment.

Could I ask that the Board and the Moderator — the one that was planned — appear in the back of the room or back in the location where we were, for further discussion.

Thank you. We hope that you will keep your seats. We have a business meeting which will, of course, go on in any condition.

Very definitely, it is not a closed meeting but it is a situation whereby as a result of pressures that we are doubtful as to what kind of contributions might be made.

TV Crew Manager: Well, it's your meeting and I very much regret the misunderstanding. I'm sorry that someone didn't speak to me since I'm in charge of the group.

* * * * *

BIOGRAPHIES

LIEUTENANT GENERAL ROBERT E. COFFIN

General Coffin's home is in Washington state. He graduated from Stanford University in 1939, and was commissioned a Lieutenant of Field Artillery from Stanford's ROTC unit. He commanded a battery of artillery in the 3d Infantry Division during the amphibious landings in Casablanca in 1942. In 1943, he landed in Sicily with General Patton's Seventh Army. In 1944, he coordinated and directed the Naval fire support during the landings in Southern France. At the end of World War II, he was commanding an artillery battalion in Germany.

From 1945-1948, General Coffin was assigned to the War Department General Staff Intelligence Division as Chief of the Soviet Branch. In 1949, he attended the Command and General Staff College. He remained at the College as an instructor. In 1953, he commanded an artillery battalion in Korea, again in the 3d Infantry Division.

In 1955, he attended the Armed Forces Staff College following which he was assigned to Army Research and Development, with successive appointments as Chief, Research Division, Nuclear Division and Missiles and Space Division. He was responsible for the staff planning and operations which led to the launch of JUPITER-C, the first United States satellite in January 1958.

In 1958-1959, General Coffin attended the National War College. In 1960, he took command of a missile task force in Italy. In 1963, he became Assistant Division Commander of the 2d Infantry Division at Fort Benning, Georgia, where he worked primarily in the tests of the air assault concepts based on large-scale use of helicopters.

In 1965, General Coffin was transferred to SHAPE as Chief of Nuclear Activities Branch. On return to Washington, D.C., in 1967, he was assigned as Deputy Chief of Army Research and Development. In 1969, he became the Commanding General of Southern European Task Force, NATO Nuclear Force, in Italy where he served until May 1971.

General Coffin is now assigned to the Office of the Secretary of Defense as Deputy Director of Research and Engineering (Engineering and Management).

He and his family live at Quarters 15B, Fort Myer, Virginia.

* * * * *

HUGH P. DONAGHUE
ASSISTANT TO THE PRESIDENT AND CHAIRMAN OF THE BOARD
CONTROL DATA CORPORATION

A.B. 1952 Boston College; M.S. (Applied Technology) 1958 University of Illinois; Service in World War II.

1952-1960 — National Security Agency; Programmer on IBM 701 and ERA 1101; Special purpose programming; Senior programmer, research in field of logical design, switching theory, microprogramming; Systems analyst, design and development of microprogrammed computer, learning process, pattern recognition, remote access; Supervisor of Systems Development Group.

1960-1966 — Technical Director, Datatrol Corporation, acquired by Control Data in 1965.

1966-Present — Assistant to the President and Chairman of the Board, Control Data Corporation; Managing Director, International Data Corporation, affiliated with International Computer Ltd., London, and Compagnie pour L'Informatique (France); Founder and Member, Board of Directors, Autocomp, Inc.

Member — Washington Board of Trade; Association for Computing Machinery; American Management Association; National Aviation Club; Touchdown Club.

* * * * *

S. M. JENKYNS
DEPARTMENT OF SUPPLY AND SERVICES
CANADIAN GOVERNMENT

Mr. [Stan] Jenkyns was born in Winnipeg, Manitoba, on August 8, 1914. He is married and has three children. He attended the University of Manitoba and the University of Nottingham [England]. From 1937 to 1939, he was employed by Rolls Royce in the United Kingdom and then joined the Royal Air Force at the outbreak of World War II, subsequently transferring to the Royal Canadian Air Force. He served as a fighter pilot and latterly in the Directorate of Air Intelligence. After leaving the service, he joined industry and eventually achieved the position of Chief Security Officer at A. V. Roe [Canada] Limited. In 1961, he joined the Department of Defence Production, now known as Department of Supply and Services where he heads the Industrial Security Division of the Security Services Branch.

* * * * *

ROGER L. CAMPBELL
DIRECTOR, GROUP 20
U.S. PATENT OFFICE

Mr. Campbell has been with the Patent Office since 1938. His duties from 1948 to 1962 were in the Security area and he subsequently served tours of duty as manager of Examining Group 110 and as Acting Examiner-in-Chief on the Board of Appeals. In November of 1970, he returned to the Security Group as Director.

* * * * *

OSCAR B. WADDELL
PATENT ATTORNEY
GENERAL ELECTRIC COMPANY

Member of the Bars of:

1. U.S. Court of Appeals for the District of Columbia
2. Supreme Court of Appeals of the Commonwealth of Virginia
3. U.S. Court of Customs and Patent Appeals
4. Supreme Court of the United States

J.D. Degree from American University.

* * * * *

MYRON W. KLEIN
ASSOCIATE DIRECTOR FOR RESEARCH AND DEVELOPMENT
NIGHT VISION LABORATORY, U.S. ARMY

Including his military service, Mr. Klein has worked in the field of night vision R&D for twenty-five years. Having completed his B.A. in Physics at the University of Rochester in 1943, he was assigned shortly after induction into the Army to serve as a physicist in the Radiation Branch of the Army Engineer Board Laboratories at Fort Belvoir, Virginia. He was instrumental in the development of the early Army near infrared equipment and, upon his separation from the Army in 1946, was awarded the Legion of Merit for his contributions.

Accepting a job as civilian physicist, in the same organization, he subsequently headed the Near Infrared Components Section, Research Section, served as Assistant Chief, Warfare Vision Laboratory and is now Associate Director for R&D of the Night Vision Laboratory.

His primary work has been in image intensification and near infrared, but from 1948 to 1952, he worked on the growing of far infrared transmitting crystals. His graduate studies at Catholic University included atomic, nuclear, and modern physics.

He has served as U.S. Delegate to NATO on near infrared and image intensification panel and has written a number of articles on near infrared and image intensification in various technical publications.

* * * * *

EDWARD J. KELLY
OFFICE OF GENERAL COUNSEL
ARMY MATERIAL COMMAND

Edward J. Kelly has been a patent attorney with the Department of Army for twenty-two years. He served with the Chemical Corps Patent Agency for thirteen years and was the Chief of that Agency at the time of consolidation of the technical services into what is now the Army Material Command. Within the Army Material Command he was appointed head of the Prosecution Branch of the General Counsel's Patent Law Division; a position in which he has served for the past nine years.

Mr. Kelly also has a military background having served in regular and reserve service for thirty years and has been retired as a Colonel in the USAR. He holds a degree in chemical engineering from Drexel University and a law degree from the George Washington University Law School. He is admitted to practice before the District Court and the Court of Appeals for the District of Columbia, the U.S. Court of Claims, and the U.S. Court of Customs and Patent Appeals as well as before the United States Patent Office. He is also a member of the Armed Services Patent Advisory Board.

* * * * *

DR. STEPHEN J. LUKASIK
DIRECTOR
ADVANCED RESEARCH PROJECTS AGENCY

Dr. Lukasik has been Deputy Director of ARPA since February 1968, and Acting Director since January 1971. He first joined the staff of ARPA as Director of the Nuclear Test Detection Office in 1966. Prior to this appointment, Dr. Lukasik was Chief of the Fluid Physics Division and Director of the Computer Center at Stevens Institute of Technology in Hoboken, New Jersey. From 1955 to 1957, he was a scientist with Westinghouse Electric Corporation where he conducted research in nuclear reactor physics.

Dr. Lukasik received the degree of Bachelor of Sciences in physics from the Rensselaer Polytechnic Institute in 1951, and the Master of Science and Doctor of Philosophy degrees in physics from the Massachusetts Institute of Technology in 1953 and 1956, respectively.

The Advanced Research Projects Agency is a separately organized agency within the Department of Defense, under the Director, Defense and Research and Engineering.

Dr. Lukasik resides, with his family, in Rockville, Maryland.

* * * * *

FRANK J. THOMAS
PRESIDENT
PACIFIC-SIERRA RESEARCH CORPORATION

Frank J. Thomas is currently President of Pacific-Sierra Research Corporation. He serves on several panels and working groups of the Defense Science Board, Defense Intelligence Agency, and others. Mr. Thomas previously was a staff member of The RAND Corporation (1967 to 1971). He served three years in Washington in the Office of Secretary of Defense as Assistant Director Defense Research and Engineering (Nuclear Programs), (1964 to 1967). Prior to this, he was with Aerojet-General Nucleonics as Manager of the ML-1 Reactor Project and Manager of the Engineering Division (1957 to 1964), and with the Sandia Corporation in the Advanced Weapon Design Group (1952 to 1956).

Mr. Thomas received his B.S. in Electrical Engineering at the University of Idaho, Moscow, Idaho, with high honors (1952), and his M.S. in Nuclear Engineering at the University of California at Berkeley, with high honors (1957).

In 1967, he received the Secretary of Defense Meritorious Civilian Service Medal. In 1963, he received the Master Design Award for the Product Engineering Magazine.

Mr. Thomas is the author of many publications in nuclear reactor technology, particle physics, and national security issues.

* * * * *

JEROME H. KAHAN
SENIOR FELLOW
THE BROOKINGS INSTITUTION

Mr. Kahan received his Master's degree in Electrical Engineering from Columbia University in 1961, after which he taught engineering at the City College of New York and worked as a systems engineer. From 1964 to 1968, Mr. Kahan served as a Physical Science Officer in the Arms Control and Disarmament Agency (ACDA). He was subsequently assigned to the Department of Defense as a member of the Policy Planning and Arms Control Staff under a one-year exchange program.

Mr. Kahan joined the Foreign Policy Studies Division at Brookings in August 1969. Currently, he is Director of the Strategic Arms Policy Study, co-sponsored by the Brookings Institution and the Carnegie Endowment for International Peace. Mr. Kahan is also a consultant to The RAND Corporation and a Lecturer in International Relations at the Georgetown University School of Foreign Service. Mr. Kahan is writing a book on strategic forces and U.S. foreign policy.

* * * * *

DR. HAROLD M. AGNEW
DIRECTOR
LOS ALAMOS SCIENTIFIC LABORATORY

A.B. 1942, University of Denver, Phi Beta Kappa; M.S. 1948, University of Chicago; Ph.D. 1949, University of Chicago.

1942-1943 — Manhattan Engineer District, Metallurgical Laboratory with Fermi group on first nuclear fission chain reaction at University of Chicago, 1942.

1943-1946 — Los Alamos Laboratory, development of first atomic strike against Hiroshima.

1946-1949 — University of Chicago.

1949-1961 — Los Alamos Scientific Laboratory, Assistant to Technical Associate Director, Associate Division Leader, Theoretical Division, Alternate Weapons Physics Division Leader.

1961-1964 — Scientific Advisor to Supreme Allied Commander, Europe.

1964-1970 — LASL, Head, Weapons Physics Division.

1970-Present — Director, LASL.

Member — Beta Theta Pi; Sigma Xi; Omicron Delta Kappa; Phi Beta Kappa; U.S. Air Force Scientific Advisory Board 1957-1968; Von Karman Study Group 1960; U.S. Minuteman Planning Group 1961; Chairman, U.S. Army Scientific Advisory Panel 1964-1970; Chairman, U.S. Army Combat Development Command Scientific Advisory Group 1965; President's Scientific Advisory Committee, Aircraft Panel 1970-present; Air Traffic Control Panel 1970; Defense Science Board 1966-1970; NASA Aerospace Safety Advisory Panel 1968-present; U.S. Army Scientific Advisory Panel 1970; American Physical Society; Los Alamos Board of Education Trustees 1950-1955; Governor's Radiation Council 1959-1961; New Mexico Health and Social Services Board 1971-present.

Award — AEC Ernest O. Lawrence Awards 1966; NASA Public Service Award 1971.

Member New Mexico State Senate 1955-1961.

* * * * *

DR. EDWARD M. REILLEY, III
ASSISTANT DIRECTOR FOR RESEARCH
OFFICE, DIRECTOR, DEFENSE RESEARCH AND ENGINEERING

Dr. Reilley is from Ellwood City, Pennsylvania.

B.S. 1940 Carnegie Institute of Technology; Ph.D. 1951 University of Pittsburgh.

Prior to World War II, two years at University of Pittsburgh Mellon Institute of Industrial Research on glass technology.

Four years military service, Signal Corps, discharged as Major in 1946. Involved in radar development.

1946-1951 Research Associate and Instructor at University of Pittsburgh.

1949-1951 Consultant to Research and Development Board in Department of Defense.

1951-1954 Fort Monmouth, Chief of Research Studies Section.

1955-1957 Assistant to the Director of Research.

1957-1958 Assistant Director of Research at U.S. Army Electronics Research and Development Laboratory.

1958-1964 Director of the Institute for Exploratory Research.

1964-1967 Assistant Director of Research, ODD R&E.

1967-1970 Director of Research and Development and Technical Planner, Post Office Department.

1970-present, Assistant Director for Research, ODD R&E.

Dr. Reilley awarded Bronze Star Medal, 1945; Meritorious Civilian Service Medal by the Department of the Army in 1964, and by the Secretary of Defense in 1967.

* * * * *

DR. ANDREW D. SUTTLE, JR.
VICE PRESIDENT FOR RESEARCH; DIRECTOR
CYCLOTRON INSTITUTE
TEXAS A & M UNIVERSITY

B.S. 1944 Mississippi State University (with highest honors); Ph.D. University of Chicago; Certificate, Nuclear Engineering 1956, University of California.

U.S. Naval Reserve, 1944-1945.

1952-1960 Senior Scientist, Humble Oil and Refining Company.

1960-1962 Vice President for Research, Mississippi State University; Director of Mississippi Research Commission, MSU.

1962-1964 Special Assistant to Director, Defense Research and Engineering.

1964-present, Vice President for Research and Professor of Chemistry, Texas A & M University.

Member — American Chemical Society; American Physical Society; American Nuclear Society; Atomic Industrial Forum; Institute of Electrical and Electronic Engineers; Sigma Xi; Phi Kappa Phi; Omicron Delta Kappa; American Security Council; Defense Science Board 1964-1969; Naval Research Advisory Committee Ordnance Panel.

Numerous patents in chemical development; numerous papers in professional journals in chemistry, neutrons, radioactivity and participation in and preparation of reports for DoD and AEC.

* * * * *

SEYMOUR J. POMRENZE
CHIEF, SYSTEMS BRANCH, OFFICE MANAGEMENT DIVISION, ASD
OFFICE OF THE ADJUTANT GENERAL
DEPARTMENT OF THE ARMY

B.S. Illinois Institute of Technology; M.A. University of Chicago.

1941-1942 — Archivist, National Archives.

1942-1946 — Army service, Staff and Faculty, Command and General Staff School; OSS, China - Burma - India Office Military Government, Germany; Vietnam Colonel, Army Ready Reserve.

1946-1949 — Records Management Specialist and Archivist, TAGO.

1950-present — Chief, Systems Branch, Office Management Division, TAGO.

Awards — Legion of Merit; Bronze Star (Vietnam); Army Commendation Medal; Netherlands Silver Medal of Honor; Honorary Instructor Awards — Army service schools; Special Recognition Citation — Administrative Management Society.

* * * * *

DR. WILLIAM J. THALER
PROFESSOR OF PHYSICS AND CHAIRMAN, DEPARTMENT OF PHYSICS
GEORGETOWN UNIVERSITY

B.S. 1947 Loyola College, Baltimore, Maryland; M.S. 1949 Catholic University; Ph.D. 1951 Catholic University.

1947-1951 — Teaching Assistant, Catholic University.

1951-1952 — Office of Naval Research, Acoustics Branch.

1952-1962 — Office of Naval Research, Field Projects Branch, Head Scientist for Project ARGUS Research, originator of Project TEPEE.

1960-1962 — Professor of Physics, Georgetown University.

1962-present — Professor of Physics and Chairman, Department of Physics, Georgetown University.

Professional Societies — American Physics Society; Optical Society of America; Acoustical Society of America; Sigma Xi; American Association of University Professors; American Geophysical Union; Washington Academy of Sciences; Cosmos Club.

Principal Awards — Mendel Medal, 1960; First Outstanding Alumni Award in Science and Research, Catholic University, 1959.

Numerous publications in professional journals in ultrasonics, lasers, solar absorptance, turbulence in light diffraction, nuclear weapons research, ballistic missile research.

Member of subcommittee of the National Strategy Committee of the American Security Council which prepared a study entitled: "The ABM and the Changed Strategic Military Balance: U.S.S.R. vs. U.S.A.," 1969.

* * * * *

DELMAR L. CROWSON
DIRECTOR, OFFICE OF SAFEGUARDS AND MATERIALS MANAGEMENT
ATOMIC ENERGY COMMISSION

B.S. 1940 University of California, Los Angeles; M.S. 1941 California Institute of Technology, 1953 U.S. Air Force War College, 1960 Industrial College of the Armed Forces.

1941-1967 — Military Service; 2d Lt. to Brigadier General, retired 1967; Bikini atom bomb tests 1946; Operation Sandstone (atomic tests) 1948; AF Research and Development 1948-1954; Office of the Assistant to the Secretary of Defense (Atomic Energy) 1955-1959; DCS/R&D, Field Command, Defense Atomic Support Agency 1960-1962.

1962-1964 — Deputy Director, Division of Military Application, AEC.

1964-1967 — Director, Division of Military Application, AEC.

1967-present — Director, Office of Safeguards and Materials Management, AEC.

Awards — Legion of Merit with oak leaf cluster; Commendation Medal with two clusters; AEC Distinguished Service Medal; Air Force Distinguished Service Medal.

* * * * *

COLONEL ROBERT B. TANGUY
USAF

Colonel Tanguy was born in Logansport, Indiana. He has a B.S. from the United States Military Academy, attended the Aerospace Research Pilot School, 1962-1963; the Armed Forces Staff College, 1966; and is a graduate of The National War College, Class of 1970.

His assignments have included duty as Operations Staff Officer, Headquarters 7th Air Division (SAC) in England to commanding the 480th Tactical Fighter Squadron at Danang, South Vietnam. Prior to attending The National War College, he was Legislative Liaison Office, Secretary of the Air Force and is currently assigned as Director of Operations, 3650 Pilot Training Wing, at Columbus Air Force Base, Mississippi.

* * * * *