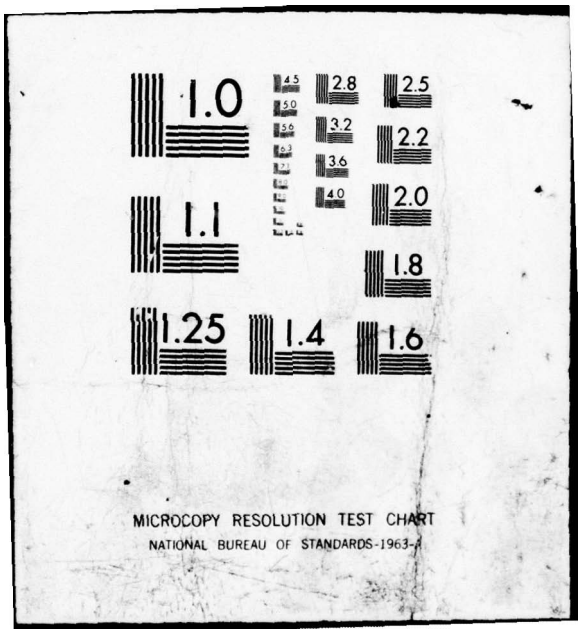
AD-A049 251 NATIONAL CLASSIFICATION MANAGEMENT SOCIETY ALEXANDRIA VA F/G 5/1
CLASSIFICATION MANAGEMENT. JOURNAL. VOLUME XIII, 1977. PAPERS F--ETC(U)
1977

UNCLASSIFIED NL

1 OF 2
AD
A049251


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

ADA049251

CLASSIFICATION MANAGEMENT

DDC
RECEIVED
JAN 30 1978
A

C
M

Unlimited

(2)

CLASSIFICATION MANAGEMENT.

Journal. Volume XIII, 1977.

Papers from the National Seminar (13th), May 10-12, 1977.

(11) 1977

(12) 117 p.

DDC
RECEIVED
JAN 30 1978
A

JOURNAL of the NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XIII - 1977

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

406 816

Published by the National Classification Management Society. Mailing address: Executive Secretary NCMS, P.O. Box 7453, Alexandria, Virginia 22307. Director of Publications and Editor of this Volume, Jack A. Robinson. Views expressed by individuals herein do not necessarily represent views of their employers nor of the National Classification Management Society.

Copyright 1977 by the National Classification Management Society

TABLE of CONTENTS

FOREWORD iii

Part One – *Proceedings of the Thirteenth Annual Seminar*

Sources, Methods & Technology – A Means to Assess the Threat 1
Dr. Jack Vorona

Science and the Technology Balance 5
Mr. Donald J. Looft

Maintaining the Land Force Capability 10
Dr. Charles H. Church

The Sea Lanes & Their Challenge 17
Dr. W. P. Raney

Air, Space & Superiority 22
Dr. Bernard A. Kulp

A View to the Future 28
Dr. James B. Rhoads

Protection and Foreign Disclosure – A Case for Balancing 32
Mr. Joseph J. Liebling

Introduction to & From Concept to Manufacture 37
Mr. James J. Bagley

The Supercritical Wing – A Case of Unclassified High Technology 38
Mr. Roger L. Winblade

Perceptions on Potential Legislation
Mr. James Davidson 38
Mr. Timothy Ingram 44

PRIZE WINNING ESSAY
Classification vs. Classi-fiction 48
Mr. Arthur E. Fajans

Patience, and the Importance of Being Redundant 51
Mr. Donald Woodbridge

Part Two – *Selected Papers*

Annual Meeting – 1977 57
Mr. Dean C. Richardson, President

Who Should Control Secrecy 60
Mr. Frederick J. Daigle

Some Background Notes Relating to Secrecy Legislation 65
Mr. Jack Robinson

TABLE of CONTENTS
(continued)

Who Should Control Secrecy in Regard to National Defense, and to What Extent? 70
Commonwealth Club of California

Society Position Regarding a Replacement Order for EO 11652 78
NCMS President Buckland

Practical Exercise – From Concept to Manufacture 87
Board of Directors, NCMS
Exercise Papers 96

FOREWORD

In this seminar we chose to re-examine the *why* of classification. True that point had been examined earlier (1969 is cited by several) but we had not returned to basics for some time. One well may ask whether our Society should be concerned about decisions of those "in authority" respecting the need for protective measures. For the very reason that we have been "coping" with such determinations since the inception of the Society; and for the very reason that wheels are "continuingly re-invented" as suggested by Tim Ingram in his comments, Jim Bagley and I – both Past Presidents -- decided that the Society should question the foundation of the system on a current basis. Are we deluding only ourselves? Is there merit in Classification Management at all? (One may note the question of Charter Member, Past President, current Counselor -- and Sage -- Don Woodbridge, "Is Classification Management the Cornerstone or the Millstone?)

One must observe also -- indeed it has been called to our attention -- that the policy aspects and procedures of the system as we know it and particularly developed extensively by the Director of Information Security of the Department of Defense, are *not* addressed in the Proceedings. This is not because they are unimportant or that we forgot them, but rather because, as stated, we believed it necessary to readdress fundamentals, and it is from fundamentals that policy is developed; not the reverse. After all, the policy for protection must be based on a *raison d'etre.* What with the published annoyance of the Fourth Estate relating to "concealments" and "denials of information" one must expect that they will lack enthusiasm for any program that limits their absolute access to whatever. Who knows -- they may be right. All they have to do is convince the U.S.S.R. to follow the same policies. One must note, however, as Dr. Vorona comments, "national means of inspection" will not open any notebooks.

Nonetheless, there is concern that the citizens of the United States be informed; a rightful concern with which all of us in the Society agree. We think it reasonable to say that we, as a Society, believe that to the extent that citizens are informed they will select courses of action to ensure that they remain free; their choice of the opposite, were it to be made, clearly would make the efforts reflected here unwarranted – if not illegal.

To the end, therefore, of serving the mutually conflicting ends of exposure and concealment we have attempted to set forth the views of those responsible and informed on the topics of concern. To whatever degree this will have been successful, we are encouraged. To whatever degree we have failed to identify the problem or area accurately, we can only express regret. To whatever degree the efforts of those presenting to cope with the challenge of our invitation provides a better foundation for understanding and interpretation for those of us who must do so, we have accomplished the desired goal.

Since the concept of the Seminar was singularly critical in this respect and was provided to *all participants we repeat it here:*

The Seminar Concept

It seems desirable to discuss the concept to be developed during the Thirteenth Society Seminar. It may be said basically to be a re-examination of the Society's stated areas of interest, emphasizing research & development.

Science – The examination of the fundamentals; developing new knowledge or amplifying existing knowledge that ultimately could provide a potential for new or improved systems. These systems may be useful in either a civil or military field or both. However, this knowledge is critical to maintaining an eminent position in world affairs. Because the application of knowledge rarely can be predicted with accuracy, extreme care must be exercised in determining whether information from fundamental research should be protected. If protection is determined to be needed, it is necessary to re-examine the decision frequently to the end that the information is protected for only such specific and limited period of time as

is warranted. ARPA can assist in clarifying views.

Technology – Wide-ranging in import and dynamic. It is important to define the terms so that a base can be established on what logically should be protected. Is it patent-like information? Is it developmental information? Is it manufacturing or fabrication techniques (L.E.D. and L.S.I. technology are examples having a myriad of applications and where the fabrications techniques make the difference between a profitable or an unprofitable operation). The areas of importance vary by application and can be best presented by the users – Army, Navy, Air Force and the Intelligence Community. The latter, for instance, can or should assess those areas of technology critical to a new or improved weapons system. Further, the place that technology plays in collection and evaluation is not properly understood and needs emphasis. It goes almost without saying that the assessment process gives further emphasis to programs in both the scientific and technological areas and this relationship needs to be understood better as to the part it plays in classification determinations. Without such an understanding there can never be a rational decision of what technology can be protected.

National Policy – This of course covers both the legislative and executive branches. What the Congress does (or does not) affects the outcome of whatever the Executive may try to do. In the Congress three aspects of current concern need coverage to assist those operating in the field to do their jobs more perceptively:

- *The Intelligence Community* – Their views, concerns and plans relating to it, whether with additional law or only oversight, are important to cover. At this time the Senate has the most elaborately constructed program and, probably, the most coherent views to present.

- *A Legislative Basis for the Secrecy/Security System* – This topic has been examined in some detail for years in both the House and the Senate. Staff members of the appropriate committees are likely best to be able to describe the views, plans and reasons. However, the absence of a legislative basis would seem to be anachronous by now.

- *Criminal Penalty Provisions* – This facet has drawn the most acrimonious comment from the media in response to efforts in previously proposed revisions to the Federal Criminal Code. What lies ahead is important to understand. It's clear that the ridiculous effect of current law – by which providing information to the media is "informing the public" and providing the same information to a foreign embassy is espionage – must be eliminated. That so few understand the relationship is demoralizing. The Senate SubCommittee on Criminal Laws and Procedures of the Committee on the Judiciary would be best to update this problem area.

Then, the Executive Program, under which a majority of those attending operate, needs to be updated authoritatively. The Chariman of the ICRC and the DASD (SP) should present information on the program and views concerning potential changes that may be perceivable by May.

Operations – Aspects of this actually will be covered under National Policy – inevitably. As a further emphasis, however, a practical exercise will be included. The orientation of its content will be to draw into focus the presentations on science, technology, and intelligence which precede. This effort is designed for policy makers, policy implementers, and bemused workers.

Three aspects of note are not going to be covered in this seminar:

- Personal, covert intelligence – its place and need have been dealt with extensively over time and are understood, one hopes, by all.

- Foreign Relations – aspects relate both to National Policy, to personal items, similarly to the above, or to other non-research and development aspects.

- Military Operations, as such.

It is felt that these have been or will be covered separately.

You must judge the outcome for yourselves. The results cannot be considered a *fait accompli*. Nothing is static. You are the critical element.

James J. Bagley
General Chairman

Jack A. Robinson
Program Chairman
and
Editor

PART ONE

Proceedings

of the

THIRTEENTH ANNUAL SEMINAR

10 - 12 May 1977

Ramada Inn of Alexandria

Alexandria, Virginia

SOURCES, METHODS & TECHNOLOGY – A MEANS TO ASSESS THE THREAT

Dr. Jack Vorona
Deputy Director for Scientific and Technical Intelligence, Defense Intelligence Agency

I am very pleased for the opportunity to talk with you in this your Thirteenth Seminar. Having said this, I must admit to having had some misgivings about being able to address an open forum on the two specific questions posed by your program chairman.

The first question was for my view concerning the impact of science and technology on intelligence sources and methods. Since it is generally agreed that sources and methods are indeed very fragile and therefore require protection (consider, for example, Senator Church's article in the 14 March issue of *The Washington Post),* I am sorely pressed to offer any specifics myself, without violating security. If you will permit me then, at least as far as the first question is concerned, I will touch upon some other facets in the relationship of science and technology to intelligence sources and methods. These facets are of considerable significance, and importance to me, and I would very much like to share them with you as well.

Quite clearly, there is a strong linkage between science and technology and intelligence sources and methods. The more advanced the technology, that goes into a surveillance satellite, clearly the greater its resolution, greater its on orbit time, the better its timeliness. To continue this, the better the acoustic sensor, the electronic sensor, the infrared sensor, the better our understanding is going to be of the threat emitter's characteristics. Moreover, as the complexity and the variety of foreign weapons systems increase, so therefore must the capabilities of our own collection and analytic tools. You might say it is a treadmill we are on, whose speed keeps on increasing. But in order to play this game successfully, there are really some fundamental facts of life we must face.

First, and as a general precept, a good science and techology machine can beat a good science and technology machine. That is, even as our collection systems improve, they can be negated in most cases at less cost than we required to build and deploy them. Since there is such a high degree of leverage involved, it is imperative that we keep our sources properly secured. I don't mean to belabor the obvious here, but this is a subject which is near and dear to our respective hearts, and I just want to mention it for the record.

Second, I believe that the day of the technological imperative is over. That is, science and technology can give us more potential than we have dollars to buy, opportunities to apply, or intelligence gaps worth the expenditure. In this regard, I can assure you that very, very tough questions are being asked relative to cost versus gain. In short, we have a technological limitation based on the economic facts of life.

There is a third concern that I want to share with you; one which has to do with the so-called bathtub effect or valley of ignorance. Figure 1 displays this effect.

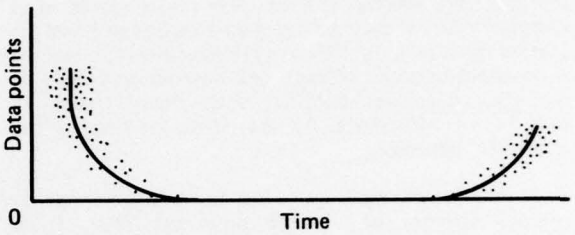


FIG. 1: THE KNOWLEDGE "BATHTUB"

Visualize an X-Y plot of our state of intelligence now versus time in any particular field of science. Initially you may find numerous data points, owing to theoretical studies in the open literature, usually with no stated or apparent purpose. As the theory crystalizes into military concept however, publications cease in time and our level of knowledge drops quite precipitously. We are now in the bathtub, and we don't climb out until the system reaches prototype testing, or worse, deployment, or even the battlefield. Because of this, the lead time we can afford our own R&D community to develop better countermeasures is, in many cases, not what we would each like to see.

What can science and technology do to mitigate this effect? Probably very little. No matter how good our capabilities, for example, they are not going to peel back any roofs, and see inside a development laboratory, much less inside the covers of some notebook. Compounding our problem still further, the Soviets are known to have a very pervasive and effective censorship system. The system filters all scientific publications destined for the open literature. And they censor, based on any number of considerations. First and foremost, obviously, they censor research if it has military application, or implication.

Above and beyond this, however, they censor a proposed article if it contains new, innovative ideas. The Soviets are evidently very much concerned about the West's ability to translate theoretical ideas rapidly into hardware or experimental results. Further, I suspect they censor, if their experimental results were obtained with the aid of instrumentation, illegally acquired; for example, perhaps there was a circumvention of Co-Com* restrictions, assuming of course, that such a connection is demonstrable.

*Consultative Group Coordinating Committee

The second question I was asked to address has to do with the effects that the scientific and technical intelligence product has had on shaping U.S. R&D Programs. Here I do have several examples to offer, although I must admit it gave security a rather difficult time for a while.

The first concerns antidotes for chemical warfare nerve agents. Because the Soviets are known to have the initiative and warheads filled with nerve agents, it is essential that we develop the most effective antidote for our troops. For a number of years we have followed the nerve agent antidote research and development done by potential adversaries. Specifically the Soviet Union, although not exclusively. All the while, looking for the innovative approach.

A few years ago, we were fortunate enough to acquire samples of one of their antidotes. These samples were compared to the U.S. antidotes for effectiveness in treating test animals exposed to measured lethal doses of a nerve agent believed to be in the war arsenal. And lo and behold, they turned out to be significantly more effective than ours. It wasn't long after these tests that their antidote formulation was added to our soldier's chemical warfare protective kit.

The second example I want to talk about, has to do with glue welding. This is the Russian designation for a metal joining process that combines adhesive bonding with spot welding. The process was developed by the Soviet Union Aircraft Industry in the early 60's. They did it as a means of joining metal sections such as fuselage panels to stringers. Glue welding was probably a fortuitous result of the Soviet's rather poor riveting technology. As you will recall, riveting is traditionally used in the West for assembling aircraft panels.

There are several glue welding variations but primarily, a high strength adhesive is applied to the lapped surfaces to be joined. These sheets are held in a fixture which is then run through a spot welder. The pressure of the electrodes forces the adhesive out of the spot welding zone and the electric current creates the spot weld. Additional spot welds are added at intervals along the seam. The second variation is to flow the adhesive into the seam after the spot welding has been accomplished. The advantage of this process is a joint that saves about 1/3 of the added weight that riveting does. For a large transport aircraft, the amount of weight saved can be on the order of 500 kilograms. In addition, the static and fatigue strengths are increased and corrosion protection is improved.

The Soviets have used glue welding on a number of transports, helicopters, and fighters since the mid-60's. Even though several of the Pact counties have been discussing this technique in the open literature since the late 60's, the intelligence community, in fact, has done a bit to bring this process to the attention of the Department of Defense, and the aircraft industry. In this country, these processes are referred to as weld bonding, and Lockheed has had an Air Force contract for the past several years to investigate applying the process to the fuselage of a C-130. I understand that the results so far have been relatively encouraging.

The third example I want to offer has to do with the closed loop liquid propellant rocket engine. Practically all previous liquid propellant rocket engines operate by tapping off a small percentage of the main propellant to operate the pump, that feeds the remainder of the propellants to the engine. This small portion of propellants that operate the pump is usually incompletely burned and then dumped overboard with all the residual energy being lost.

Now one way of increasing the efficiency of an engine is to increase its operating pressure. However, when you increase the operating pressure of the main engine, the pumps themselves require more energy to pump the propellant into the main engine. This reduces in turn the amount of propellant available for the primary ignition and increases the amount of waste energy. Eventually, you can reach a point of no return where you are actually wasting more energy than you are burning. There is, of course, a way to recapture most of this wasted energy. Instead of dumping the portion of unburned propellant overboard, it too can be forced into the combustion chamber. That is, closing the loop so that all the unburned propellants are consumed and consequently, all the end product energy is fully utilized.

This is a simple concept, but it was the Soviets who actually realized it in the early 60's. We are rather certain they were doing this, but didn't know for sure until much later. To date, the U.S. has not successfully flown such a system, but it is scheduled for use onboard the U.S. space shuttle. With this concept, engines can operate more efficiently at higher pressures, yielding a 3-10% increase in specific impulse, which is quite considerable when you are approaching the absolute in chemical powered rocket propellants. That last few percent, as you know, is usually very difficult and very expensive to attain.

A fourth example I would like to cite has to do with the Soviet's BMP. When the BMP was first deployed in 1957, it was the first operational serially produced mechanized infantry combat vehicle or MICV. The unique system characteristics include integral anti-tank missiles, an automatic loader for a 73 MM gun, the capability for mounted combat as witnessed by firing ports; a chemical, biological and radiological protection system which allows the troops inside to function without gas masks, and a low silhouette with a very sleekly, radically sloped armor plate for increased protection.

Although BMP components and engineering design have not been copied by Western designers, the vehicle itself has influenced the criteria for MICV performance capabilities in the West. For example, the use of anti-tank guided missiles along with main gun armament for an anti-tank capability, as evidenced by the Federal Republic of Germany's MADER Vehicle; a radical slope of the French AMX-10P's upper glacis armor and its radiation detection alarm. Firing ports on the MADER, the U.S. MICV and the Italian MICV. Since the BMP's deployment, transported troop mounted combat-capability has become a standard feature of almost all MICVs.

Parenthetically, I would note that this is one of those items that we didn't see; we had no inkling about it until it appeared in a Moscow parade in 1967. The bathtub got us on this one.

I would like to now cite the case of the Soviet PMP ribbon bridge. The PMP ribbon bridge is their current standard tactical floating bridge. The bridge set provides materials for constructing 745 feet of class 60 bridging; that is, bridging capable of handling 60 ton loads. During their recent maneuver, a combined Soviet-Czech team assembled a 650 foot PMP bridge in 15 minutes, a rate of over 40 feet per minute. The normal rate of assembly, however, is assessed at about 20 feet per minute in currents moving at about 5 miles per hour. One of our service intelligence units, the Army's Foreign Science and Technology Center at Charlottesville, performed an evaluation of the Soviet PMP bridge and presented briefings on the systems operation and capability to the chief of Army engineers in 1969 and the commanding generals of the Army's Readiness and Force Development Commands. These people were very impressed by the capabilities of the bridge, as well they might be, and of its obvious advantages over any similar bridge that the U.S. had in its inventory. Subsequently, a contract was established with the Pacific Car and Foundry, and a prototype developed. The prototype proved successful, and the Consolidated Diesel Electric Company was awarded a contract to produce 300 of these systems.

Then as a result of the 1973 Arab-Israeli War, several pieces of Soviet PMP bridging equipment came into our hands. Study and analysis of the equipment resulted in our improving, upon the original PMP bridging, both in its design and manufacture. For example, the U.S. variant is made of aluminum versus steel, resulting in a considerable weight savings. Estimates computed by the Army Corps of Engineers revealed that better than $50 million in R&D and prototype acquisition was saved by copying many of the design features of the Soviet PMP bridging in the manufacture of the U.S. version.

The area of Electronic warfare is my last case in point. The Chairman of the Joint Chiefs of Staff in his Posture Statement noted that the electronic warfare posture and readiness of U.S. forces are marginal to meet the threat posed by the Soviet and Pact countries. This assessment resulting from recent comparisons of our electronic warfare capability and those of the Soviet Union identified a deteriorating balance between ourselves and the Soviet.

The 1973 Mideast War furnished new scientific and technical intelligence on Soviet communications, electronics, and electronic warfare doctrine and tactics as well as equipment. In light of the Soviet electronic warfare threat then, we have evaluated our weapons, our command, control and communication systems effectiveness and have initiated programs to overcome deficiencies.

The susceptibility of field equipments is being determined, and where practical improvements are underway to make them less vulnerable. We have also taken the initiative to train, devise tactics and define procedures in ECCM -- electronic counter countermeasures -- in order to complicate the Soviet's task. In fact, a DoD directive in May, 1976 has been issued directing the incorporation of the ECM capability in the design of new electronic hardware. Moreover, this directive specifically requests DIA provide the system developers the threat data necessary to better focus their efforts.

I must admit to considerable satisfaction in this, since it clearly recognizes and formalizes the important role of intelligence in the weapons system acquisition process. There is one additional item I want to bring to your attention. And it has to do with the receptivity of the U.S. R&D Community to ideas and hardware generated elsewhere, primarily the Soviet Union. Several examples I just cited, clearly represent the situation where scientific and technical intelligence were taken to heart by the R&D community. And by the way, I would note that it also suggests that intelligence is being obtained and furnished to the consumer with a need to know.

Unfortunately, the openness of others in the R&D community, to outside ideas, leaves something to be desired. For a long time, the Soviet Union was indeed technologically backward, and we saw them field large numbers of systems so as to overcome deficiencies in quality. I think the situation is rapidly disappearing, but many of us still seem to cling to the security blanket of our technological superiority.

This residue of times past may account in some measure for the "not invented here" attitude within a segment of our R&D community. A classic recent example relates to the Mig-25 Foxbat which landed at Hakodate Airport in Japan. When it was first examined by some of our folks, there were exclamations of disbelief, because there were actually roundhead rivets

seen protruding from the fuselage. As it turned out however, the roundhead rivets were only in those places where the airflow boundary layer was quite thick, and therefore they didn't significantly affect the aerodynamics of the aircraft. On the other hand, the rivetheads were flush where it did matter. I suspect one could develop a very interesting philosophical discussion on just what does constitute technological superiority, or sophistication.

Ladies and gentlemen, I wish to thank you for allowing me to contribute to your program. I would be happy to entertain any questions that you have.

Questions and Discussion

Question: Would you care to comment, Doctor, in terms of your evaluation of our protective system of classification in this field? Do you think our system is effective in protecting in the R&D community was necessary to the development of the kind of system that you address.

Answer: You are catching me outside of my area of expertise by asking me to comment on the effectiveness of U.S. classification systems, on U.S. developments. I feel rather uncomfortable doing that, and rather unknowledgeable in the field. The openness of our society no doubt results in the release of considerable R&D data. This however, is a price we should be prepared to pay.

Question: On the subject of technology exchange with our foreign allies, how do the people in the State Department, in ISA and in the various agencies find out from you what they know about us. Do you have an interchange of information? Do you have a method of advising the State Department, the ISA, and the military departments' -- Army, Navy, Air Force -- foreign disclosure people, what the Soviets know about us?

Answer: Yes. I don't know if it is as effective a mechanism as might be. I am sure there are significant improvements that can be made to make sure that nothing falls between the cracks. However, we do work very closely indeed with the State Department and the Assistant Secretary of Defense for International Security Affairs, on virtually every critical piece of technology and software which might be sent overseas, either to the Soviet Union or some countries in the Bloc. We do work very, very closely, and provide our assessments as to the possible gain or loss of each piece of critical technology or equipment or software which is proposed for sale overseas.

Needless to say, our recommendations are not always taken.

Question: When you receive intelligence information that relates to compromise of information or classified material on which a defense contractor is currently performing, do you have any method by which your people tell us that fact? That certain information has been compromised and treated as unclassified? In essence what I am saying is, if the information has been compromised and an intelligence activity so reveals, the contractor in a lot of cases is still protecting it and impeding performance on the program. Is there a way that you can or do make the contractor aware of this?

Answer: I really can't answer that question since it's not within the purview of the intelligence community to declassify R&D data.

Question: Are you aware of any method or procedure within government, which can define or establish what technology is of interest to the national defense? There are Offices of Technical Assessment hither and yon -- there is one in Congress too, for example, and there is the Presidential Science Advisory Committee and others. But, is there any means by which you can say, yes, this bit of information is or could be useful to the National Defense?

Answer: I think we are beginning to take some steps in that direction. What we have done in DIA for the past nine or ten months is to set up what has been referred to as an advanced technology panel. And the purpose of this panel is to discern which are in fact the critical technologies to the Soviets. What we have done is to do individual case studies, whether it be ballistic missiles or aircraft, or land warfare, or electronic systems or directed energy weapons -- the whole spectrum of systems which have military consequences. Starting with the individual warfare system, we branch out to its components and the various contributing technologies. Eventually, you come upon a technology which is truly critical, one which the Soviets would have to either develop on their own or get from us in order to make some kind of a substantial improvement in their system's performance. Having isolated these technologies, we would then be able to go back to the Department of Defense and/or State Department and say, these are truly critical and we recommend that suitable arrangements be made to preclude their compromise via technology transfer.

The first study will be out on the streets in about a month or less, actually, and it has to do with directed energy weapons. By September, we hope to have the remainder done. They will treat virtually all the military systems of consequence.

We think that this kind of an effort will better allow us in our job of providing support to ISA, to better focus on what should be really denied export in

the national interest, and what can be exported with relative impunity.

Question: Is there anyway that DIA could communicate to defense contractors specific areas of subject matter which conceivably at that particular time, could be of interest in terms of formulating the weapons system or something along those lines? Specifically, my problem is, in the case of independent research and development reports, essentially, one looks for military application but engineering tells me everything has a military application. Often it is a very fine line between what is and what isn't classified. Can DIA advise or provide contractors in some way with some general idea in subject matter terms of those of special interest or sensitivity at a particular time? Even if the information was classified, it would be a great help in reviewing IR&D reports.

Answer: I would have to answer, from my perspective, no.

Question: Are the studies you mentioned going to be available, or to whom are they going to be available?

Answer: They will be available primarily to the people within the intelligence community, and will be classified of course; it is my understanding that we will make it available to all the consumers in DoD and throughout the rest of the community who have need for it. I might say there is another consumer who has evidenced considerable interest in this publication, and that is the resource people. These studies should tell us, for example, where to put our diminishing analytic resources. In sum, the answer to your question is, it will be widely disseminated throughout the intelligence community and to the consumer community.

Question: Would you imagine that this effort -- which appears to be in a relatively early stage -- will come to the guidance kind of concept that the Society has been promoting? Offering cautions about what really needs to be protected most, by dissemination through the user agencies and their distillation and further dissemination to laboratories say?

Answer: Absolutely. We intend to make copies of these available to people in ISA and the State Department who are routinely involved with such items as technology transfer.

Question: Would this approval perhaps cause the United States to work more closely with NATO allies in developing future weapons because of highlighting the information areas needed or not needed by the Soviets?

Answer: I don't see the connection between technologies critical to the USSR and your suggestion that we work more closely with our NATO allies. But there is a mechanism to control the flow of technology to the Soviets. It is the so called CoCom mechanism. This is the International Coordinating Committee which is charged with the regulation or the monitoring of sales materials to the Bloc. The CoCom nations include all of NATO, exclusive of Iceland and it also includes Japan. Now this is not a treaty and therefore, it doesn't have force of law behind it. But diplomatic and other kinds of pressures are brought to bear, within this CoCom community to make sure that critical technologies, *etc.*, are not in fact, sold to Bloc nations. It doesn't work in all cases, but this mechanism does exist.

Question: Your examples were directed at the Soviet Union. What about the technology of Communist China. Do we learn anything from that?

Answer: The chances are possibly, yes. I am sure when you put 750 or 800 million people to work, something innovative is going to result from it.

It might be that instead of a CDC7600, there are five acres of teenagers pushing abacuses around. I don't know. The problem here is that if the Soviet Union is considered a relatively closed society, then the Chinese are a clam. And we just don't have that much insight into what is really going on. I do note that there was a rather traumatic break in Soviet-Chinese relations in the early 1960's. I would say most, if not all of Chinese technology up to that time had been of Soviet origin. Or at least the philosophy was of such an origin. Since the break, the Chinese have had to move out on their own. We do see some instances where they have gone off in new directions but as far as having sufficient insight into their programs to say, we can benefit from that or this or this, I am afraid the evidential base just isn't there.

SCIENCE AND THE TECHNOLOGY BALANCE

Mr. Donald J. Looft
Deputy Director
Defense Advanced Research Projects Agency

The process of identifying, designating and controlling information or knowledge – as I prefer to think about it – that is of national interest, is certainly of vital importance to our nation's defense, as well as our economic well-being; and the two are becoming even more inter-connected these days. It is also a very complex task. I congratulate you on your past accomplishments with which I have personally had considerable familiarity. I further congratulate you on having meetings like this to stay current in what is a fairly dynamic field.

As you know, I represent DARPA, and, in brief historical comment, you may remember that it was established by President Eisenhower. One of the things that you may not completely realize is that DARPA in many respects, is like a central research activity of major corporations--such as IBM, Texas Instruments, RCA, or General Electric--which despite the existence of R&D activities in operating divisions, still have a central research facility and activity. The Secretary of Defense, like his corporate counterparts, has need of a flexible research capability such as DARPA, reporting at the highest levels and committed to high risk, hopefully high payoff objectives that are at the cut-off edge of technology. At least we like to think so. Such a facility is not encumbered by institutional biases, by roles and missions restrictions or other such constraints.

To give you some idea of the nature of current DARPA programs, we have organized our activities into what we call major thrusts. Very briefly, these are concerned with space defense, space surveillance, anti-submarine warfare, undersea vehicles, armor and anti-armor initiatives, command and control and communication. Another — perhaps unique — is lowering the cost of defense. Then finally, some efforts--seed efforts, if you will--aimed toward future technological revolution.

A basic DARPA mission is to minimize the possibility of technological surprise in the context of advanced technologies. One of our concerns is inadvertent offshore transfer of information that represents technological gains or advantages which we may enjoy over other nations, with a *quid pro quo* or a discernable advantage to be gained. In view of your information management mission, I believe this subject is of interest and should be of concern. Certainly, in the next year or so, you will hear a lot more about this topic as new policies and new procedures begin to emerge. Today, therefore, I would like to talk about this topic, emphasizing some of the basic issues involved and identifying some of the actions that are being taken now to address this problem.

First, however, let me digress and perhaps philosophize a bit. Peter Drucker--one of my favorite authors--has stated that the only real resources, any organization has are money and knowledge. If you think about this statement you can see that in the broadest sense, it clearly is profound. The question then is, from a national viewpoint, how do we manage these basic resources?

The Department of Defense, among many, expends considerable effort to manage our money resources. Though I am sure there are many who don't always agree, I think we do a reasonably good job of it. Money resources are easy to measure or count; they are highly visible; and all of us, from our earliest upbringings, are sensitive to their allocation to achieve the greatest utility, as we individually perceive that result. Knowledge resources, on the other hand, present a much different set of problems. My experience suggests that as a nation, we often do not recognize our store of knowledge, or information, as a basic resource. We probably do not manage and allocate that resource as well as we might. We certainly do not expend the same level of effort to manage and utilize our accumulated knowledge as we do our money. Furthermore, there seems to be a tendency to view knowledge as a sort of an omnipresent service. It is much like the indifference we have to the water from our faucets at home. It has itself seemingly little value until it suddenly stops.

This situation is not too hard to understand if one considers the intangible nature of knowledge or information. It can't be counted or measured; its value is highly transient; and quite often it is very difficult to recognize. In reality it is a heterogeneous mixture of objects, people, documents, drawings, models, ideas, experience and the like. Accordingly, it is a very difficult resource to quantify and manage. In fact, it may happen--as you have heard, I know--that attempts to manage knowledge may stunt its growth, and shorten its life.

With that philosophical foundation, I would like to turn now to the manner in which we handle or trade or consume that portion of our knowledge resource we term technology — particularly, the offshore transfer of technology. Why is this issue important? What is the nature of technology that is of concern? What are the mechanisms by which it may be inadvertently transferred? What are the current control procedures? And, what new approaches are being considered to improve our national advantage without adversely affecting our economic wellbeing.

The technological advances we have represent the fruit of a long term national investment both commerical and governmental. They are a vital part of our national security posture, and are essential in maintaining our nation's economic wellbeing. The technological gains we have made are the keystone of our national productivity and, in turn, our wealth, our strength, and our standard of living. Technological advantage is represented by a host of forms of knowledge ranging from an understanding of a basic physical phenomenon to a myriad of how to do, how to build details. Technological advantage is not a steady state condition. Rather, it is generally characterized as a highly transient state with forms of knowledge having very great velocities of change.

These latter factors compound the difficulties of identifying and controlling a technology that is important for a given time frame. To compound the problem further, particularly from a national defense

viewpoint, many technologies serve defense and non-defense needs equally well. For example, the basic silicon chip technology and the universally available pocket calculator can be applied to missile guidance; numerical controls for machine tools; or a number of important signal processing tasks. Despite these complications, we must be careful that we do not over-react and assemble a firing squad to dispose of this problem--it would be undesirable to form them in a circle. We want and we need to exploit to the fullest, our comparative technological advantage in doing business with other nations. At the same time, we do not want "to give away the store."

Considering technological information, what is the most important ingredient? Is it advanced research and development? It is products that embody advanced technology? Is it design data? What is it? What are we trying to protect? During the past year, a task force was convened by the Defense Science Board, in response to a request from the Secretary of Defense to analyze export control of technology from a DoD perspective. Mr. Fred Bucy, the current President of Texas Instruments, chaired that task force, which included senior people from a broad segment of industry and government. These experts examined in some detail, four representative high technology industries--solid state electronics, instrumentation, aircraft jet engines and airplanes. I would like to quote from their principal findings--they are pretty short and pretty succinct.

After examining the entire technology spectrum from basic research through maintenance of the finished product, they found and we concurred that transfer of design and manufacturing know-how is of overwhelming importance to our national security. Mastery of design and manufacturing processes increases a nation's capabilities. It is in this area that the U.S. maintains its technological leadership. Think about this a bit and I believe you will come to the same conclusion. It is a sound and sensible finding. I suspect your own experience in information management would show that design and manufacturing know-how always represent the most proprietary data. These findings of the Defense Science Board's *ad hoc* committee emphasize that, from a national viewpoint, the control of design and manufacturing know-how is absolutely vital to the maintenance of U.S. technological superiority. All other considerations are of *secondary importance.*

This task force then examined the manner in which technology is transferred inadvertently. It asserted that there were three types of exports, which transfer manufacturing and design know-how most effectively. These are ways of design and manufacturing information that includes detailed "how-to" instructions on those processes. Keystone manufacturing inspection or automatic test equipment, and products accompanied by sophisticated operations application or maintenance information. Note the lack of emphasis on product *per se.*

While the task force's perspective was that of the DoD, and properly reflected concern for national security implications, I think their findings are fundamental and should be of interest and concern from the standpoint of our national and international economic posture. Since your membership is concerned directly with the broad spectrum of governmental information as well as with private information--which may be disseminated at home and abroad--I believe these findings are of interest and include factors you may very well need to consider in the future, and undoubtedly will, as new policies are promulgated.

To give a frame of reference: under present export procedures, most items fall under the general license category. That is, a company which negotiates a sale of items in this category simply completes a shipper's export declaration, which is provided to the Bureau of Customs for determining export fees; the Census Bureau for data purposes; and the Department of Commerce's Office of Export Administration, for review against commodity control lists. Most of the commodities on these control lists are there because of national security interests. For the general license category, once the seller has filed his export declaration and paid the requisite fees, he may go ahead and ship the material involved. If the material, or a key element of it, is on one of the control lists (*e.g.,* the U.S. Strategic Control List, or Allied Strategic Control List--the so-called Co-Com List) and the shipper has knowingly violated that list, he is subject to penalty. In most cases, exporters are familiar with these lists and routinely make application for a special export license if a controlled commodity is involved.

The application is reviewed by all the federal agencies, and ultimately either the Department of Commerce or the Department of State, if the item is on an admissions list, issues the requisite license or disapproves the request. Obviously the Department of Defense is one of the key agencies in this review process, because of the controlled material that may be involved and its national security implications.

To give you some idea of the magnitude of this kind of an activity, the volume of requests for export licenses that flow through the Department of Defense number in the thousands every year. Current procedures require a case by case review generally focusing at the product or system level. These detailed reviews pose a number of problems for the shipper, with their inherent time delays and uncertainties. It is difficult to carry out an aggressive sales effort, and be responsible to a potential customer if he is not sure he can legally deliver the product. Further, these determinations do not provide guidance for the future and the reviews

tend to focus on the wrong issue in light of the DSB's definition of the most important form of technological information.

Products, clearly may not be the critical issue. Therefore, current thinking with regard to export control of technology is to emphasize key elements of a technology, including critical production processes and key manufacturing equipments and de-emphasize control of products *per se,* excepting critical items of direct military significance. For example, we are not going to sell the Russians guns that give them a direct, immediate capability to shoot at us. But in a related vein, we are also very concerned with the processes by which weapons, say, can be produced in volume automatically. There are active efforts, currently throughout the Executive Branch of government, to develop new policies and procedures that reflect the general approach I have been describing.

Within the DoD the Secretary of Defense late last year, assigned the Deputy Director for Research and Engineering the responsibility for re-examining all current policies and practices, regarding offshore transfer of technology. A priority effort involving the assembly of a task force of people to carry this out. Their main objectives have been, I believe as of this week, largely completed; first to identify and maintain a composite list of technologies and end products--existent or in research and development--with revolutionary military, as well as civilian technology potential, which are recommended to be protected. Then, they have been concerned with identifying military and military-related technologies and products which the U.S.S.R., its allies, and the People's Republic of China need and want. They are also concerned with the net technological or techno-military assessment in order to provide a list of technologies and products to be considered for export control by the U.S. and by its allies. They have also attempted to determine and maintain foreign capability in the free world, to produce these technologies and products. The lists of categories of products and technologies recommended for export control, are for consideration of Commerce and State Departments.

Once these objectives have been met, implementing policies will be prepared and of course, the data and policies that have been established utilized to review and process requests for export licensing. These new approaches should insure that technical parameters of concern are being considered; that the stated end use is appropriate; and that licensing history for the product and end-user is considered. In some cases, one would expect that products previously denied for export may be approved. Also, some former denials may now be approved on foreign policy or economic grounds.

To emphasize the difference between products and technology, let me give you an example that perhaps some of you are familiar with. One of the requests that the United States has had in many forms from friends and allies is for detector assemblies used in an infrared detection and imaging system. Under previous policies, we would have been very reluctant to approve requests for allowing a manufacturer to ship the detector assembly, *per se.* If you examine that problem a little bit, what you find is that the key information involved is all the details associated with processing that detector; how the crystal is grown initially to get the proper mixture of metals – if it is a tri-metal detector; it is delineated on the substrate; what kind of anti-reflection coatings are put on it; how it is mounted on a cryogenic cooler; how the connections are made to the detector to bring off the electrical signals; *etc,* You could hand the finished assembly to someone, and let him use it. The real issue is not the item but the manufacturing know-how that provides the capability to produce more such items. The investment in reverse engineering that the recipient would have to make to achieve the capability would be very large. That is an illustration of the difference between products and technology. I don't think there is any question--based on the Bucy report--from a national viewpoint, that our future policies will be much more likely to go ahead and sell him that detector assembly.

Obviously, there are limits. We are not going to sell 10,000 of them to a potential enemy so that he can equip his entire force and shoot at us at night. However, the point is that we would not be nearly as reluctant to sell him a number and still be confident that we really have not given away the store. On the other hand, we have been able to market a technological investment to our national advantage. But there is a distinct and perhaps somewhat subtle difference between the way that problem has been approached in the past, and the way it is intended to be approached now. Hopefully, we will be smart enough to do that properly. Of course this is a very difficult problem area and the determinations will not be easy. People in your business are going to be right in the middle of them, because it is the management of information or national knowledge, that is of vital importance to us.

I have attempted to tell you briefly about this current problem. As I indicated, I think and I hope it is of interest to you. The procedures that are being developed right now should make it much easier for manufacturers to compete in world markets and market products abroad, and at the same time, minimize the possibility of our inadvertently transferring technology that is part of our national store. In the past, we have been fairly generous with our technology. Often, we have been willing to sell it very cheaply since the investment required to generate it had already been recovered in U.S. markets. Those days of generosity have got to end. The time for hard-nosed dealings to recover a fair price, even with preferred trading partners, is at hand.

On the foreleaf of this report of the Defense Science Board (the Bucy report that I mentioned earlier) they were clever enough to include a quote, by a world renowned author named Vladimir Il'ich Lenin. You may have heard of him. He said,

> "The inherent contradiction of capitalism is that it develops rather than exploits the world. The capitalistic economy plants the seeds of its own destruction in that it diffuses technology and industry. Thereby undermining its own position. It raises up against itself foreign competitors, which have lower wages and standards of living and can outperform it in world markets."

Need I say more on the importance of technology transfer to our national well-being? I may have turned up the contrast a little bit, but I think the statement is well worth recognizing and thinking about.

The theme of this seminar stresses the need for a re-examination of national policy and operations as regards management of information relevant to science and technology. Let me assure you that in the matter of offshore transfer of our national store of information--that which gives us technological advantage--there is a serious re-examination underway. I believe it will yield a much more effective and enlightened policy and responsive procedures to insure we exploit to the fullest, any advantage we may enjoy.

You as professionals in the management of information will undoubtedly be important contributors, to the lengthy and sometimes tedious processes necessary to meet our national objectives in these regard.

Questions and Discussion

Question: I couldn't help noticing, listening to your remarks, that there is a little contrast between your presentation and Dr. Vorona's this morning, in that Dr. Vorona gave us numerous examples where the United States is able to get the products rather than technology and proceed from there to make up a technological event. Whether this simply means that the United States is superior in that way, or that there is a philosophical difference that one should consider, I don't know. Do you have any comment?

Answer: I think that is a good point. I think all we are saying here is that if one furnishes products to someone, and that someone makes the required investment, he may be able to convert that product into a manufacturing or design know-how; that's true. On the other hand, he may not. But, we don't want to hand it to them. We have made quite an investment in many cases, to develop particular design and manufacturing know-how to enable us to effectively produce certain items in quantity. What we are saying in this instance is, keep your eye on the donut; the design and manufacturing know-how is the important thing. Don't get hung up on the sale of a few products. Usually it is to our economic advantage to do that, and we do not lose--in the near term at least, we would not lose seriously from a technology transfer position.

Being insensitive, as an alternative, has resulted in cases such as those where industries have gone ahead and set up whole factories because it was good business; but from a national viewpoint, it was the worst thing they could have done. A related problem is found in some instances of factories having been set up in friendly nations who subsequently have sold them to unfriendly nations; the whole factory, that is. One of the greatest advantages the U.S. enjoys in the world is our advantage in solid state electronics, integrated circuitry, and high density electronic circuits. And we have sold a factory to somebody. That doesn't mean we gave them the best technology that we had, but we gave them quite a leg-up.

It's true that none of these things are ever black and white. But, my whole purpose in coming here today, and my interest in talking to you, is because you really have the problem. The management of technological information is a tough problem. Many feel that one simply reviews a list, and selects from the list. Either you do or you don't. Well, it doesn't come out that way. Those answers are never that clean. There are times when you want to say yes, and there are plenty of times when you should not say yes. Even if all the indicators would suggest you should.

Comment: Your presentation was most encouraging because it reflected enlightened attitudes by the Department of Defense, and they will do away with a lot of our fears that what we have been doing in the past is forcing Europe and Japan to create their own technology.

Response: That's right and is a very good point. That is one of the reasons why the problem was looked at this way. We do not want to do that. We want to make our products sufficiently attractive, because it is a tough world out there. It is the United States that is no longer able to maintain its economic posture, to maintain our standard of living, *etc.*, unless it competes for those world markets. If we don't, you know somebody else will be out there doing it for us.

Comment: Another point that may need mentioning is that by licensing you can control where information is used and how it can be used, and where it might be employed. This is a terrific advantage for us.

Response: That is an excellent point, and I am sorry I didn't mention it. Licensing is a technique that does exactly as was indicated, and one that is used widely and should definitely be exploited.

Question: Your presentation included economics as an important element for consideration. What is the long term posture of the United States economically in competition with both our friends and our potential adversaries?

Answer: Well, I think that the United States in the next ten years will emerge into a national economic posture which will make it very strong in the world. I think we have learned that we do not have unlimited resources. We have learned that we cannot be autonomous. We have learned that we have a serious energy problem. In my view, I sense that our whole citizenry is sort of re-awakening with a spirit that I think was unique to this country in its early days. Puritan ethic is beginning to emerge again a little bit. You know, if you want to eat, you have got to work, and if you want to compete, you have got to put out. In the end, that is what is going to make the difference.

Question: Let me rephrase the question. Do you think we will be No. 1 in ten years?

Answer: I think we will be very hard to beat. Is there anybody who is a very strong contender?

Question: You touched upon an area that ERDA has been pretty much concerned with, and I infer from what you said that the DoD is realizing that the classification management world is becoming technically more sophisticated everyday. Am I correct in inferring that the DoD realizes that in fact classification management business has to become technically more sophisticated in order to be able to differentiate between those areas when providing the hardware, is basically the same thing as providing the manufacturing know-how, and those areas where we can safely provide the hardware without then providing the manufacturing know-how?

Answer: You are absolutely correct. In other parts of the Bucy report there were statements to the Secretary of Defense to the effect that he has a problem. That if he wants to solve the problem, he must allocate some resources, and get some professionals into this business. You cannot make these kinds of determinations with clerical personnel.

Question: Are you describing technical professionals?

Answer: I am describing people with technical orientation who are professional information management type of people. I don't know exactly what that means. The Department of Defense is taking steps to create spaces, create jobs, because if you are serious about doing this, you have got to do it right. Otherwise, we are back where we started.

MAINTAINING THE LAND FORCE CAPABILITY

Dr. Charles H. Church
Assistant Director for Technology
Office of the Deputy Chief of Staff, RD&A,
Department of the Army

Our potential enemies have very strong land forces. An Army fights on the land – or should we say it fights with equipment that is normally land based – against primarily land based targets. So, I am not really going to talk about technology so much as I am the problems that the U.S. Army may have in fighting in the next five to twenty years. Remember that the battle area may not necessarily be the NATO area.

I have two tasks today, first:

- To exercise a crystal ball to try to tell you just what the future might be like. I have to do this in my professional capacity in the extended planning annex, which presents what the Army is to spend its money in the ten years beyond the next five year defense cycle. We have to come up with what kinds of systems will be needed and what technology will be required to develop them.

Second, and even more difficult:

- What is going to be classified, or what is classified

I tend to classify what we have now and what we are currently capable of, and not classify what is in the future. Knowing the way the system works, among other things, I am never sure what we are going to be able to buy in the future. However, I do know that what we have right now, may have significant limitations.

I consider myself three different people: an optimist, a pessimist, and a realist. To define: An optimist is one who says that he is hoping. A pessimist says that he is not really hoping much. As a realist, I would say that the tank we are going to have in 1990 is a tank a lot like we are going to have right now. It might be the XM-1, it might be the XM1A1 E2, or something like that. It is probably going to be a lot the same. It will probably be nearly the same tank in the year 2000.

The helicopter won't look much different either; for example, quite a few people have a great deal of difficulty in telling one Army weapon from another. The rifle looks much the same. There are some that think the M-16 does not vary much from a M-1903

Springfield. One has a little bolt on the back and the other does not, and one is a little bit lighter. This is true as well of many of the Army's weapons - they are very similar in appearance. Parenthetically, that is one of the reasons we have trouble in buying new ones. If you go to a soldier, for instance, and tell him that I want to sell you this new "thing," he may say, "that looks the same as my old 'thing' and it costs five times as much. Why should I buy it?" As a scientist and a technologist, on the other hand, I say that there are going to be some major changes that may not be visually apparent to the casual observer. So, I would like to talk about some of those major changes.

- **ENERGY** An area of major change is this old question of energy. We are speaking of the energy cost of existing....existing as an armed force, existing as a country. The installations cost (which turns out to be major) of the military forces is the energy expenditure in just heating and cooling necessary buildings. As we begin talking in terms of about a dollar or two for a gallon of heating oil its cost can be forecast to take a much larger fraction of the current budget and even more so in future years.

- **MOBLITY** We really do not know where the next war will be fought. We assume that it might be in NATO. However, Vietnam did not happen in NATO; the Arab-Israeli war did not happen in NATO; for one or another reason, there are going to be many regions of the world in which the United States may have a military interest.

- **COMMONALITY** An area that we hope to see change more is that of expendables. Insofar as possible, we would like at least to have common expendables with our allies. By an expendable, I simply mean a rifle bullet, a fuel, or a cannon projectile. An example of non-commonality is the large number of different guided missiles used by the NATO countries.

- **TECHNOLOGY** Some technologies have rapid rates of change. We have some major questions on how the potential enemies handle their equipment. What are their limitations? An area where there is going to be, and has been, major change is the whole field of computers; we have the mini-computer, the milli-computer, the micro-computer, and macro-computer.

  As time goes by, you will be less and less aware of the presence of the computer, but if you try to achieve a certain capability without having the computer, you would fail. You will be finding computers in air conditioning systems. You will be finding them in your car; we will find them in many more of our military systems.

- **SENSORS AND DATA LINKS** Of the four speakers this afternoon, at least three of the speakers have a background in electro-optics. All of us had known each other before this afternoon, so it shows that the sensor, at least in the Department of Defense, is getting some attention.

Some goals towards which we are moving are shown in figure 1.

FIGURE 1

GOALS OF THE LAND FORCES OF THE FUTURE

- **High state of readiness**
- **Nearly independent of weather**
- **Capable of operating in most terrains**
- **Kills are effected at longer ranges**
  – Beyond enemy capability
- **One shot, one kill at high rates**

One of our most difficult problems is maintaining our readiness. We have to be able to go to war on moment's notice. For example, one of the current postulates on how a war would start is that it would be from a training exercise. The fighting part of the Army has to be prepared to wage war at a moment's notice. We say a moment's notice which may be six minutes, six hours, six days, or even six months.

We have to be able to operate nearly independent of weather. Some of you are old enough to remember a war called World War II. During World War II, there was the Battle of the Bulge. The time for that battle was chosen by the enemy to be a time when the aircraft were standing down because of weather. The stand-down essentially negated the U.S. Army Air Force which was then our most mobile anti-tank force. We could not really mobilize our resources, the land resources, rapidly enough to cope with his initial thrust. As you know, with luck on our side, and a few other things, we finally did stop him. Perhaps he could have really gone all the way if he had more strength, and had really been able to maintain his momentum.

Consider the term capable of operating in most terrains. In the first part of the Vietnam War, the United States Army found out that the jungles were not like Europe at all, that things like fungi and so

forth tend to grow; the bugs were bad, but also the soliders themselves found all sorts of new diseases, and new ways of getting these they had not thought of before. The most important asset for an army is the people, and they must be in shape. So when I say most terrains, I mean both militarily and also medically. You have to be able to feed them, you have to be able to let them sleep, and they have to be able to operate.

Even though the enemy will be choosing the time and place the United States wants to be able to wage the war under our terms as well as we can. We would like to be able to affect the kill at longer ranges because the closer you are to being one on one, the less chance you have of surviving.

So, the longer the range at which we can kill, the farther we can get beyond his capability. For example, current tank fire control systems are based on a combat range of one to two kilometers. We would like to have our combat capability based on two to three kilometers or more. Because of logistic problems, if for no other reason, we would like to be able to have our future systems have one shot, one kill.

Figure 2 shows some limitations on achieving these goals. One of the major limitations on achieving these is a simple one: "Who do you shoot at?" On a map you can draw a red line, but in reality, that red line does not exist. How can you be sure that the guy coming at you isn't one of your own tanks withdrawing. He will not be able to buy you a beer in the evening if you kill him with your one shot, one kill equipment. So, as you change over to the smart weapons that can effect one kill with one shot, then the question of who is a friend or who is a foe becomes more important. I tend to think that that first problem tends to be one of the pacing problems in the application of smart weapons.

FIGURE 2

LIMITATIONS ON ACHIEVING THESE GOALS

- **IFFON: Identification, Friend, Foe or Neutral**
- **Personnel: Operating & Maintenance**
- **Logistics: Having sufficient stocks, particularly precision guided munitions (PGMs)**
- **Philosophy**
  - **One on one; need one on many**
  - **Compartmenting of functions**

Then, how do you train the people to use these weapons? A major problem is that we cannot afford to have the soldiers fire the weapon that they are going to use in combat training. For example there is one weapon, the Armor Piercing Discarding Sabot (APDS) round, which is considered to be the tanker's primary weapon. I was talking with an armor officer, a colonel, who said that he has never fired it. The APDS is used in the M-60A1 tank, and will be used in the XM-1 tank. Why not? Simply because there is no range large enough in this country to allow you to fire the round in training even though this is to be the major killing round for the tank in the future. Further, you cannot afford to fire many guided missiles because of their high cost. You have a couple people who are in a platoon that are trained to fire a Dragon or a Tow anti tank missile. The others have not fired the missile. But in a real wartime situation, they may be required to because the trained soldier may be sick, he may be on KP, he may be digging a foxhole, or he may be dead.

Another major problem in logistics is having sufficient stocks, particularly of precision guided munitions. Those of you that were acquainted with what happened in Vietnam found that SA2's and SA3's were being fired at 4-5-6, 8 and 10 rounds per target. If you have an expensive round, you have to really worry about the husbanding.

The philosophy that I show as a limitation in figure 2 is addressed to how we think out wars. In general, the current way of thinking of a war is one tank takes on another tank, and then has it out. You cannot afford to fight that way. You are then fighting the battle on his ground. What you have to think is that one weapon system can take on two-three-four-five or ten at one time. This requires some rather sophisticated thinking, as well as some sophisticated planning, command, and control.

Another philosophical limitation is this whole question of compartmenting of functions. This is both compartmenting in the intelligence sense which I call the "Green Door" syndrome and compartmenting in a functional sense such as anti-tank and anti-air. We now have separate little groups of people to do each of these tasks.

Figure 3 deals with classification and I'll offer some views as aspects covered. I would tend to classify equipment that is nearer at hand as opposed to further away. We would like to classify the weaknesses of our systems. In many cases, we really cannot, because the systems that are deployed, that we have right now are so old that everybody knows the weaknesses, because everybody in the world owns them.

FIGURE 3

WHAT DO WE CLASSIFY

- Particular weaknesses of a weapons system
  - ours
  - knowledge of theirs
- Specific technologies having great military promise: HEL, PGMs

HOW DO WE KNOW WHEN TO CLASSIFY

- The developer
- The User/Operator

We also classify our knowledge of their systems. We classify in this case a weakness on our part. We really do not know as much as we would like to know about any enemy system such as a tank. We would like to know of what kind of steel it is made; what the power plant is; about the transmission; and, we would like to know its reliability so that we could estimate how many they are going to have effective at any one time. We would like to know their advantages for a three man crew. We would like to know why they picked the weight that they did when all the rest of the armies of the world are picking a different weight entirely.

Very quickly, we would like to know a lot more about their philosophy in planning and choosing weapons. What we are really asking, "What are their caveats. What are their constraints? What are their driving forces?" These are obvious questions. We do tend to classify specific technologies having great military promise such as high energy lasers, and precision guided missiles.

Turning to "How do we know when to classify," the usual source we go to for classification is the person that develops the weapon. We assume he may know what is classifiable by virtue of his knowledge of the state of the art. We also go to the user or the operator in the Army, to ask what they think is classified.

In figure 4 I have shown some aspects of the Soviet Union forces, since they are considered to be our primary military opponent. They are heavily armored. Their tank to man ratio, their armored vehicle to man ratio is probably the highest of any army in the world. The Soviet division of 10,000 men has as many tanks or more, actually, depending on the kind of division than the U.S. division, which is nearly twice as big. But they have other problems than we have and they have a wholly different philosophy of operation. He is highly mobile, on the ground and through the air. He is very highly sophisticated, in his uses of available engineering - not science - engineering. He is highly sophisticated in some technologies and lagging in others. His biggest area of sophistication, may be just a plain old processing of steel *(e.g.,* the electro-slag cast steel, and electro-slag remelt steel.). He tends to be a very good steel founder. His computer work, his sensor work, his chemical work, even his engine work, appears to have a lot of deficiencies. For instance, we have not found yet the presence of a turbocharged diesel engine in a Soviet combat vehicle even though this is standard western technology. Almost every truck that is being made in any western country right now has a turbocharged diesel engine. As far as we know, he has not yet incorporated it. If you want to make a high power to weight ratio diesel engine, that is one of the ways to go.

FIGURE 4

SOVIET UNION: THE OPPONENT IN EUROPE AND MIDDLE EAST

- Heavily armored, heavily armed
- Highly mobile: Ground, airmobile and airborne
- Highly sophisticated in use of his available technology: steel processing
- Lagging in other technologies:
  - Computers – Macro thru Micro
  - Chemicals
  - Engines
- Major land forces are fifties, early sixties design generation
- Major reequipping in progress

By chemicals, I do not mean chemical warfare. He is very good there. I mean just plain old bulk chemicals - the plastics world - the world of polyethelyne. I think what drives our country is the consumer market more than the military market.

He is currently going through a major re-equipping, a major modernization. He is about five years ahead of us in this modernization, perhaps even more. He is, we are finding, fielding completely new families of vehicles.

In figure 5 I present some of his military advantages because I am talking about the land force capability and that is the U.S. Army's major concern. He is close to the action. Most of you probably have not looked at a map recently. But it is the same distance from Israel to the Persian Gulf as it is from Soviet border to the Persian Gulf which is about 600 miles. In order to

do anything there, he would have to mount the forces. That is true. But, he can do so completely inside his borders.

FIGURE 5

SOVIET UNION MILITARY ADVANTAGES

- **Geography: He is close to the action in Europe and the Persian Gulf**
- **Quantity: He keeps everything and produces large numbers**
- **Quality: His deployed equipment is effective when properly used**
- **Standardization:**
- **Timing: He calls the "Time to go"**
- **Engineering: Conservative, single minded approach**

The Soviet Union does not throw anything away. He produces in great quantity and the material he produces is good. His deployed equipment is very effective. I think his current family of self propelled guns is probably as good as exists in the world. His 122mm gun is about the overall size of our M113 personnel carrier; a little bit bigger. However, it is amphibious which is unusual in a self propelled gun.

So, I do not want to frighten you but I am simply saying, we have a problem. He makes the rules on standardization. His weapons can be fired by his allies. He has the timing. He can say when to go.

When We consider comparable U.S. military advantages, the list is rather short.

- TECHNOLOGY
- RELIABILITY
  (A major subset of technology)
- PERSONNEL

Our technology is an advantage even though it is primarily of the commercial world and not deployed in the U.S. military forces in any great quantity.

Another major area that the United States does surprisingly well in, even though a lot of you may not think so from your cars, is the whole question of reliability. In general, the U.S. products, military products, on the world market, is the standard by which other products are judged – be they Soviet, German, British, or French. The United States in general, does an extremely good job of fielding a reliable weapon of war. And as you know, unless a weapon is going to work reliably in wartime it is not much good for anybody.

Then as to personnel; as you go over to smarter and smarter weapons, you need smarter and smarter people. That is unless we get really smart and figure out how to make smart weapons that are employable by people who are not quite so smart which requires a very high level of smartness.

Figure 6 lists some major problems faced by the U.S. and its allies. One of our biggest problems is that old question of readiness as I discussed previously. Another problem, particularly for the U.S. Army, is modernization. How do we get our more advanced systems out in the field and how do we get them out more rapidly, but still reliably? How do we take the products we have in the field and improve them.

FIGURE 6

MAJOR PROBLEMS OF US AND ALLIED LAND FORCES

- **Readiness: We have to respond**
- **Modernization:**
  - **New systems**
  - **Product improvements**
- **Standardization and Interoperability**
  - **Language problem alone is bad**
- **Mobility:**
  - **Strategic**
  - **Tactical**

Another problem is standardization and interoperability. For example, can we file the same information, use the same fuels, and use the same equipment? Right now, there are telephone systems, military style, in each of the different allied armies that really do not interconnect too well. They do not intercompile, they do not interoperate, and very few of the different countries have people who even speak the different languages. For example, how many of you speak French, German, even British, fluently? You can see how this could adversely affect command and control.

Once more, the question of mobility. The Army's major way of getting around the world is the C-5, which is gradually getting grounded. It takes a tremendous amount of transport to be able to transport a single modern division overseas. A standard planning assumption is, that the equipment will be there when we want to use it.

Let us turn now to the contributions of science and technology to the solution of some of these problems. In figure 7 some of the elements are presented. How do we take advantage of what we have, and how do we create those new weapons of the future, but in a workable way? The United States is emphasizing the computerized approach, the electronic approach. We are working on sensors, on radars, and on command and control problems. The modern weapon system, be it a fighter, or even a tank, is an electronic marvel.

FIGURE 7

WHERE DOES SCIENCE AND TECHNOLOGY PLAY A ROLE

Current Trends

- **Improving combat capability**
  - **US is emphasizing electronic approaches to improving capability**
- **Decreasing costs in acquisition & operating**
  - **US is making major efforts to reduce combat manpower**
- **Improve human effectiveness**
  - **Personnel**
  - **Training**
  - **Fitting the tools**

The Soviets are emphasizing something slightly different but quite a few of their new weapons systems tend to emphasize reductions in combat manpower.

Then, how can we make the machine fit the man better? I once defined a smart weapon as one that works in combat with a man using it rather than a scientist or a good technician. So this involves both the choice of the personnel, the training of them, and also as I mentioned earlier, the fitting of the tools to the people. If you are to have people with an IQ of 90 operating your equipment, you had better make sure the equipment fits the people with the IQ of 90.

Moving to figure 8 we see more roles for science and technology. One of the other functions of a scientist in the Army is to identify the strengths and weaknesses of ourselves and others. He also provides the capability to analyze new technology such as when will a precision guided missile work, and when not? He must be able to tell the operator not to put all of his hopes and dreams in that new thing; he had better have a fallback position. That is also a role of the scientist. This is one that does not get done well enough, because the scientist and the operator are not talking enough together. By the operator, I mean the soldier in the field as opposed to the soldier scientist, who quite often tends to sound like a scientist rather than a soldier.

FIGURE 8

"WHERE DOES SCIENCE AND TECHNOLOGY PLAY A ROLE?"

- **Forecasting improved capabilities**
  - **Identify strengths and weaknesses (US and others)**
  - **Analyze impact of new technology**
- **Improve older systems**
- **Develop new systems**
- **Market new technologies**
  - **Some times we do well: Thermal imaging**
  - **Other times, not so good: Laser beam rider**
- **Intregrate new technologies into army**
  - **Change over**
  - **Training**

One of the other things that we should do is to tell him how to improve his old system. You do not have to come out with a new tank to put a new fire control system on it. You can put a laser range finder on the old one, and it will have better fighting capability. That is pretty obvious, but it is very difficult to tell people. It is also our function to try to figure out what new system will be beyond the current system as well as the generation beyond that. And then, figure out how to use it.

The term market in figure 8 is used in the sense of convincing people at all levels that we should put our money into something. We have done a very good job of selling thermal imaging systems. I think everybody is convinced that the thermal imaging is the way to go. But there are other areas that we have done a poor job of selling, with the laser beam rider being an example. We have been bandying it about for 4-5-10 years.

This ability to be able to see a technology, to push it, and to get it into a new system is a very, very important job for a scientist engineer, and it is probably one of the most difficult jobs that we have and one of the biggest. One of the roughest parts about it is cost. New technology in general is expensive, and if you bring in new technology, you are talking about doing it for all the forces.

And so there is this question of the integration of the new technology in the army, and also the training of the people to use that technology. Training people and the training aids can be more expensive than the fielded device. Let us turn now to some of the technology opportunities that may enhance our land force capabilities. Figure 9 presents some of them.

FIGURE 9

WHERE DO SOME TECHNOLOGICAL OPPORTUNITIES LIE THAT WILL ENHANCE THE LAND FOR CAPABILITY

- **Sensors:**
  - **Matrix focal plane arrays: "Super smart eyes to see in the dark and through smoke"**
  - **Millimeter & submillimeter radiometry & radar technology**
- **Guidance**
  - **Infrared imaging: Cost is the big bogie**
  - **Supersonic & hypersonic laser beam riders**
  - **Laser gyros**
- **Materials & material design**
  - **Armoring**
  - **Composites**
- **Computers of all sizes; explicit and imbedded**

The first listed sensor started partially in industry, partially at the night vision lab of the Army. It is coming back into the Army. It gives us the promise of making a smart sensor. I am not talking about a smart weapon; I am talking about an eyeball that can think. We are putting a computer in an eye. We can tell it what it should recognize. We can tell it to distinguish a tank from an APC or from a jeep.

The second has been a technology lying in wait for a long time. The submillimeter wave technology is a spinoff of the laser technology.

In the guidance area, infrared imaging is, as noted, very costly and that is a major problem. The supersonic and hypersonic laser beam riders are for a new anti-tank missile. We also need technology in acquiring and identifying the target as mentioned previously. The last guidance item, the laser gyro. is slowly creeping into military systems. Then in materials – a promising area is armor. You may have thought that this was a settled matter but the XM1 tank is an example of new armor. The composite material area may be the wave of the present, the future and somewhat the past but it is where our newer structural trends are to be. As you will notice, many of these technologies do not seem to involve the computer explicitly. However, I think almost every item up there, one way or another, has a computer somewhere in the background, just like there is always a mother in the background. The computer almost is the mother of new technology, if for no other reason than because it tells you how to choose what to do. The computer may be explicit or imbedded; inherent as an aid to design; to computer-aided manufacture; to computer-aided tests, and, to computer-aided budgeting.

Then moving from the technology to the resulting systems, figure 10 lists some that I think are going to be developed. The lightweight, heavily armored anti-tank air defense fighting vehicle (a move away from the existing compartmentalization problem to which I referred), and the highly maneuverable and high speed helicopter. I tend to think that helicopters have a long way to go before they peak out and become asymptotic. Asymptotic is when a technology peaks out and there is nothing more to do. For a long time, as I commented, we thought armoring was in that category. Then suddenly, something happened which is realized in the XM-1 tank. The helicopter was thought to be in that category, and I think this has changed.

FIGURE 10

SOME POSSIBLE FUTURE ARMY SYSTEMS

- **Lightweight heavily armored at/ad fighting vehicles**

  Highly maneuverable high speed helicopters

Both with target forecasting ability and high killing rate potentials

- **Armored artillery systems capable of shooting on the move, and auto loading and reloading**
- **Nearly invisible remotely piloted target acquisition systems that work**
- **Surveillance, and target acquisition systems (active and passive) that are coupled into near real time communication, command and control systems**

Then advanced technology systems can provide advanced information on both where the target is, and what the target is doing. Artillery can be developed that can fire on the move and can be almost completely automatic. The real problem may be how to make it reliable. I also can see that the nearly invisible remotely piloted vehicle (RPV) can be made. If you made an RPV of a translucent material and backlit it or internally lit it, it would be optically invisible against the sky.

Some day we are going to learn how to tie all these sensors together, via computers, and be able to present the enemy order of battle and the electronic order of battle to the local commander or even to a front line soldier in a near realtime fashion.

Then, what are we doing to tie all this together? The Army is trying hard to do a better job of managing its resources and the following are some major management innovations:

- **MANAGE BY CAPABILITY CATEGORIES**
- **SCIENCE AND TECHNOLOGY OBJECTIVE GUIDE – (STOG) UPDATED ANNUALLY**
- **MANAGEMENT SUMMARY SHEETS (MSS)**
- **ADVANCED CONCEPTS TEAM**

The first of these is that we have divided the Army budgeting into combat capabilities. For example, we have grouped the tank systems and the anti- tank systems. We are also grouping them in our science objectives. We are trying to focus more and more intensive management attention on the system as currently being developed, the system as fielded, and the system as it would be considered for the future. And hopefully, we are also cross-talking among these. The science and technology objectives guide (STOG) is a new thrust that we have put together to have in one book objectives that the developer and the user can agree upon as to where the Army ought to be going. Then, we have the management summary sheet, where we present on one piece of paper all the work that we are doing, for example, in tank technology.

Further, we have created the advanced concepts team. We have the temerity to tell people and run ads that say "bring in your idea; we will judge the idea; and if we think it is good, we will fund it." Probably 75 to 90 percent of the letters we get the person has not given sufficient thought to what he is talking about to be able to present a reasonable discussion of the idea. But, the other ten or twenty percent contain surprisingly good ideas; ideas that would have trouble finding their way into the Army or the services without this kind of help.

To summarize, the United States Army is fielding the best land force we can put together within the budget. We are trying to develop the best land force within the budget constraints. We are as open as we can be to ideas. If any of you have any ideas, bring them to us and we will get them a hearing even though you may not like the answer.

And, lastly, I have no simple formula for classification.

Questions and Discussion

Chairman: I cannot resist a comment. I am dating myself when I make it. Two of the prime vehicles of the Army, the jeep and the 2½ ton truck, were adopted over the objections, and believe me, over the objections of the old Army Ordnance Corps. I know all of the people involved who fortunately are still living.

Second, if you want to find out about submillimeter radar, talk to a guy named Merril Skolnick at NRL.

Question: What is the program for metricization? Using the metric system.

Answer: Bit by bit by bit. In the XM1 for instance, there is a requirement laid out as a result of an agreement on parts with metric units. I happen to feel very strongly that the current industrial trend in the United States toward metrification will be a real boon to us in inter-operability and standardization. I think that the United States being almost the last holdout on English units is really hurting us. I do think that it is not just inertia. It is that people hate to do something different. But the Army in our new systems is specifying metric as much as possible.

Question: How sensitive is the Army towards the area of fiber optics.

Answer: We have a program in fiber optics at Fort Monmouth. Our program in fiber optics is more towards long telephone lines, taking the place of the hard wire, rather than in internal communications such as in a tank. We have a program using a fiber optic data link to a missile. This program is one in which the missile as it flies out, deploys a fiber optic that then serves as a video data link.

Question: The reason I asked the question is on account of the fact that other agencies or other DoD components treat the area of fiber optics as relatively sensitive.

Answer: Right now, the Army, as far as I know, does not. Last year, in the corporate report, we broadcast widely our work in fiber optics.

Question: Is the Army getting ready for an automatic across the board declassification of all equipment and information relative to that equipment that was abandoned in Vietnam?

Answer: I do not know!

THE SEA LANES & THEIR CHALLENGES

Dr. W.P. Raney
Office of Science & Technology Policy
Executive Office of the President (on loan from the Office of Naval Research as Deputy Chief of Naval Research & Chief Scientist)

I haven't prepared slides for this talk, which means that I must either talk about exciting things, or involve the audience, or both. I would prefer, however, to get you involved, for you are the poeple who are actually

dealing with classification problems and know far better than I what are the problems worth time and effort.

In our preliminary discussion about what the topic should be, it quickly became clear that the questions were:

- What is the future of the Navy to be.
- What will be the important areas of science and technology.
- How do we recognize what items from those areas will need protection and require classification procedures?

I will start bluntly by saying that I don't know what are going to be the most important scientific areas.

I can't think of a major war in a long span of history that failed to depart radically from what people thought it would be. That is the nature of wars. Between wars, everyone plans according to a particular set of scenarios, and the next war is always different. With the rate at which science has been progressing for the last 50 years or so, we know that we can't see what the scientific knowledge, or indeed the usable technology, is going to be for anything like the mean time between wars. I am, of course, talking about central war between major powers, not the hundreds of limited armed conflicts that flare up every year.

Whatever our difficulties in prognosis, we must still try to move ahead in areas where we think there may be advantage. What I want to do this afternoon, therefore, is just to make a few remarks about areas that are clearly going to be of general interest to the Navy, and about items that we should recognize so we can be quick about exploitation and not wait too long for the new possibility to be proved in practice.

The Navy has a great many functions, with many roles and many missions. All of the services do, but I will assert that the Navy has a particular challenge in being required to operate variously above, on, and below the surface of the ocean, and through the Marine Corps we must be able to conduct amphibious operations. Occasionally, as we found in Viet Nam, the Marine Corps must operate almost entirely on land, in which case it is not much different from an army. This scope of mission in turn requires a technical scope that is very broad -- enough so that the number of technical items is hard to handle.

All of this comes under the general umbrella that covers the operations of all the military departments: the business of strategic deterrence. A fair share of our national resources is devoted to maintaining the deterrent posture, and it is beneath this primary function that all of the conventional military operations take place. I personally think that the concept of deterrence operates also at levels well below that of strategic issues, applying thereby to major conventional confrontations. We do force-level studies on the required number of capital ships, the number of submarines, aircraft, and so forth -- and what those forces mean in terms of net advantage or disadvantage. The conventional force balance is clearly a play of deterrence in much the same sense as in the nuclear case.

There are peculiarities about the classification problems associated with strategic deterrence. The capability must be real, but since the world has never had a nuclear exchange, this genre of warfare is theoretical. There are many experts in this theory, and many very complicated projections and scenarios, but hard facts about what constitutes significant damage to the United States in a security sense are elusive. For as long as strategic deterrence is operating, damage from a security leak is largely in the political and public relations arena. I hasten to point out that unwanted leaks of information about strategic deterrence could ultimately cause a substantial change in the national posture, but fortunately it has yet to be demonstrated that leaks have an effect on the outcome of a battle.

Thus the classification problems are peculiar. Judgements about whether to classify something very highly, or not to classify it at all, become rather sophisticated, because part of the practice of maintaining a deterrent posture is that we want the other side to know in considerable detail exactly *what* we can do in the event of war. The one thing we don't want them to know is *how* we do it, for if they know, it might be possible to devise a counter with some new device or tactic -- and then our ability to deter the other side would in fact be damaged.

The result of the need to advertise our capability results in some surprising things showing up in the public domain; obviously they are there because it has been decided that we want the other side to know what we can do. Obviously we need to protect very closely what the vulnerabilities of our system are and what are the technical bases for our capability. But our capability, or selected portions of it, moves very quickly from great secrecy to full publicity. That is the way deterrence works.

Strategic nuclear war is at the top, but as we move down the scale toward major conventional war and some of the traditional Navy functions, we must somehow cover the intermediate ground. An element of that intermediate region is the topic of tactical nuclear weapons. No one can be sure they ever *will* be used, but we must plan around the fact that they *may* be

used; we must act as if they will; and their capability must be real. But generally, because I think people believe there is a slightly greater chance of using tactical nuclear weapons, the security is more opaque for them than it is for the major strategic system, where we want the other side to know and be afraid.

Let us now try to see in a few general themes what our projections of future tasks for navies and for the Marine Corps may entail. We start with the fact that communication is very rapid, transportation can be pretty fast, we aren't at all sure where the next armed conflict is going to break out, and we don't know how quickly we will be asked to respond. All this argues that there will be a high premium on flexibility, on mobility, and on detailed command and control. We learned some of these things very well (some of them again) in Vietnam. There was obviously a considerable problem with trying to engage in warfare in the middle of a civilian populace; there were problems of identification, problems with sensing enemies, and problems with precision guidance of weapons. The details of our technical approaches to the solution of these problems were immediately important, and the need for security protection was great.

Let us look at another facet. The Navy does not expect to be heavily engaged in land warfare beyond the operations of the Marine Corps in amphibious warfare and whatever duties may be assigned to the Corps ashore. However, there is still the matter of supporting the projection of force ashore, which entails a large number of functions. The classical view of what it takes to win a war include occupying territory and controlling it. The Navy is clearly a means to the end of getting people ashore in quantity. If you must have people ashore in quantity, we don't have the aircraft assets for that, and we certainly don't have the aircraft assets to deliver the supplies in quantity. But the Navy supply assets are limited too, so we must depend on civilian bottoms if the conflict lasts long enough to require substantial resupply. All this means that the Navy will still have to be involved in the classical functions: convoying, arranging for the control of commerce so that it is free to us on the surface, antisubmarine warfare in order to protect its own assets and to protect the support for forces overseas.

I would like to express, at this point, a view that raises another peculiarity which classification management must face. Just as seagoing warfare is becoming increasingly sophisticated, warfare on foreign territory is becoming less clear. How such warfare should be waged and whether one can really make a convincing demonstration by landing and controlling territory has been put into considerable question. Even if you nominally control the territory, there is a question about whether the war is going to be over. This means that the whole area of public relations, political pressures, economic pressures, need for raw materials and supplies -- all these become ever more important. They have to be taken into account in any military thinking. Most of the information dealing with that sort of subject is not classified, unless it is a high-level summary. But suddenly the perception may change and the information will become highly classified.

Let me give you an example. The Navy has a medical laboratory in Cairo. It has been there a long time; it is an excellent establishment and has served as a strong tie between our governments. One of its functions is to work on what can perhaps be classed as public health measures against diseases that we might encounter in that part of the world. That work has made the laboratory valuable to the Egyptians, and they have cooperated by providing us epidemiological statistics. However, during the period of open conflict between Egypt and Israel, such statistics were determined to be of strategic importance, and we no longer got them. There was no question about some exotic disease that someone might consider a potential weapon in a bacteriological warfare sense. It was the everyday working material used in the research program that suddenly changed its character and became highly classified. Similar shifts in attitude between war and peace could easily occur for meteorological information.

To return to our discussion of the world in which the Navy will find itself operating, I repeat that it will be a world in which we have few assets, and a very sophisticated set of functions. Thus the Navy will have to depend on its wits, and it will need technical help on some of the problems. The technical response will have to be quick, and it will have to be good. In turn, there are some implications for the handling of classified information which I shall discuss later.

Warfare appears to be heading into a period when the offensive side has a very distinct advantage. That advantage comes about through the use of sensor imagery and the sort of missile control and performance that has now been demonstrated for all to see. We have known about such capability in prospect for a long time, but demonstrations are much harder to ignore than are theoretical projections. The fact is: cruise missiles can hit surface ships. Cruise missiles have to be detected from beyond the line of sight so we can knock them down. Or we must play the uncomfortably sophisiticated game of keeping track of all potential launch vehicles, estimating their intentions, and attacking them between the time they are committed to attack us and when they actually do it. As a nation, we don't make the first move in starting a fight, but we can certainly get all tangled up in trying to tell -- long enough ahead to be alive to do something about it -- when an enemy is going to fire!

With few assets and troubles likely to pop up anywhere in the world, the Navy is going to require much

greater capability in world- wide surveillance than it has had in the past. At the moment, that requirement obviously means satellites. It is going to need sophistication and data rates in its command and control greater than it has ever had in the past. Thus there will be a high premium on solving some of the two-way data flow problems, which will involve secure and possibly covert communication -- and *high* classification requirements. On the other side of the coin, capability in surveillance by the opposition will be such that the traditional Navy ability to go and hide in the far reaches of the ocean, even in daylight, is badly degraded. It is not completely gone -- as any task force commander who has played games with the opposition can tell you -- but it is certainly nothing like as good as it was several decades ago. If you can't disappear by sailing over the horizon, then the whole business of electronic warfare, of trying to confuse the opposition surveillance while protecting your own ability, will become very important.

Electronic warfare is a measure-countermeasure game, and it has traditionally used equipment that is pretty close to the forefront of what technology can do. Everyone must adapt and respond very quickly to what the opposition is doing. It is expected, and it goes on all of the time in electronic warfare. The time for coupling between new science, new technical capability, and the deployment and use in the field is much shorter than it would normally be in other areas of military operations. That is a situation where one would expect that the desire to keep classification wraps on rather basic science information would be extraordinary. That is true, but just as the very important strategic deterrence information finds itself in the papers for good and sufficient reason, this area of electronic warfare, which depends on very quick response and very quick introduction of new technology, is one which most of the community is willing to share with our allies. The exchange is often much easier for electronic warfare topics than it is in some other areas of military technology. It is a curiosity, one of the several I have mentioned today.

Another dominant feature of warfare in the future is small unit fire power. It is staggering. That statement goes for all the branches of the military. Army small unit fire power is greater than ever before. This facet, too, emphasizes the importance of surveillance systems that can keep track of everything on the field, because even the little fellows can kill you now.

I would like to mention just one more view that will argue still further for the importance of flexibility and quick technical adaptation. Our traditional modes of military planning and thinking about the roles, missions, and style of equipment are not so much opposed to that the Soviets employ as they are orthogonal. I say that in the sense that the Soviets start with the basic philosophy that they are going to protect their homeland, and any fight is going to be a quick, violent fight. Their vessels, their Navy ships, at any rate, don't have any great resupply capability. They expect either to win or lose, early on. If they must get back home for resupply, they don't have very far to go, since the basic purpose was to protect the homeland.

Now, however, they have started building naval vessels that have considerably greater distance capability. We see them in any part of the world. And they have a lot of ships, which means they now have the capability to do more than simply protect the homeland. It is not at all clear that it is their intent to do more than protect the homeland, but they now have the technical capability to indulge in adventurism. That is a worry for everyone, because their ships are good ships, they can stay away from home, and they are equipped for quick, violent fights.

Most of the U.S. planning, on the other hand, is based on a different philosophy. If we can't deter a fight, we work for the long haul. First of all, we try to keep our wars away from home, so the ships have to be able to go long distances. It is expensive to come back and get supplies and repairs, so our ships are made with some capability for forward support and repair afloat.

There is an asymmetry in the situation that is rather difficult to handle. We usually think and have thought, based on our experience in World War II, Korea, and Vietnam, that we can hang on for a while; our industrial capability can come into play; and we can build up our combat capability. But if our basic philosophy is consistent with a long war, and the Soviets are planning on a short war, there is a problem. The success of an *initial* engagement, may determine whether we will have the time to build -- as we have in earlier confrontations. The success, if it is that, will depend on our sophistication, our flexibility, and our grasp and ability to use the latest in science.

Now let me wind up with a few remarks that pertain to the problem of how we stay flexible enough, and how we get the good, tight coupling between military operations, new technology, and new scientific knowledge that is going to be so important. Also, we should discuss when you classify and when you do not.

My first remark is that every once in a while I run into a point of view that says, "If we don't tell people something, *they* will never think of it." I hear enough chuckles to make me believe you agree that it is an idiotic proposition. It is idiotic for several reasons. One is that a hallmark of science is a high degree of internationalism. Not only is there wide publication and discussion in the domestic part of science; it is totally international. Over and over again, if you look

at the history of science during periods when there have been flurries of advance, you will find that the whole world, at the least the scientific world, is like a ripening vine. Time after time, when someone notices a significant new discovery in science, you also find that within a span of six months or so, there have been three or four or five people who have, more or less independently, discovered whatever it is. This is so because areas of science or technology tend to be of interest and, therefore, active at particular moments in time -- worldwide.

Thus anyone who picks up a great new *thing* and decides that it has obvious importance and should, therefore, be classified so as to give us a lot of lead time is deluding himself. This is partly due to the fact that sooner or later someone else will think of it, but if the item is truly important and at the forefront of science, several other people around the world are going to publish or announce the news very shortly.

Science, an activity on which we will ultimately and do now depend, absolutely must have public disclosure and scrutiny. It must be challenged. A characteristic of science is that it challenges itself internally all the time. Science is not very good at selling itself or selling new ideas, because the whole culture of the scientist is to try and understand, to test an idea, to challenge it. Not sell it, *challenge* it and see whether in fact it is true. The way science progresses is by having external challenges and external scrutiny. Thus, any time science is kept from that sort of public scrutiny, it is going to wither and slow down.

Now it is perfectly possible, in time of war, that the national good says we should shut science off from public scrutiny. We can't make much progress in science *per se* during a major open war anyway. But until we are in an open war, we want to keep our scientific community healthy. We cannot stifle it by stopping public disclosure, because that is what it lives on.

Let me digress for a moment and say why I think we classify things. One reason is to prevent people from knowing what our operational capability is. As I have said, in strategic deterrence, we do just the opposite. Another reason for classification is to keep people from knowing that we are trying to develop an operational capability. Normally, that reason is pretty solid, and we do it most of the time. However, in SALT negotiations we have a cruise missile to talk about and there is a great deal of publicity about our trying to develop the capability. Third, we classify because we want to buy time for development. That is the area that is usually most difficult, for we don't really know how much time we are buying. I have suggested that if the item is at the forefront of science, we buy essentially no time at all. The place where we can buy time is when we can recognize the application before the opposition does and don't talk about it.

Occasionally there are major programs that are very highly classified, very highly technical, at the forefront of science, engaged in instant application and reduction to practice. There is usually a tight little community that knows about it. By and large, I would say that the sponsors of such programs are successful in hiding the existence of a certain capability for a while. By and large, such programs are extraordinarily expensive and extraordinarily wasteful. Moreover, they stand a very high chance of going wrong, because they don't have the public scrutiny and argument and challenge that is the essence of the best in science and new technology. Someone makes a decision and the system gets to work in a hurry, with attendant real problems. Any decision to go "black" with a program that involves high technology is a decision that has to be taken very seriously for it is too easy to hit wide of the mark.

Sometimes such decisions provide elements of humor. During the early days of gas-dynamic lasers, I went to visit a plumbing and heating contractor to hear about a special-access development of such lasers. The company was well organized for visitors. They had never had a limited access program before, and never in the history of the company had they had so many visitors and given so many briefings. It was the best advertising they could possibly have had. It was rather like being banned in Boston. My more serious point is that sometimes limited access works for cases in which the stakes are very high. But restriction is a costly and risky business in the early technology and high science area.

There is another question very close to a lot of arguments about classification or other control. It is the question of government ownership. A few years ago I talked to a commercial firm that was interested in a new type of engine, using a novel working fluid, carbon dioxide. They thought there was a chance of real commercial profit, but they needed to know more about the details of carbon dioxide near the triple point. They had done some theoretical calculations of the sort one usually finds in reference books, such as the *International Critical Tables.* They had a lot of new data points and they were holding them company proprietary. I was astonished. Proprietary information about carbon dioxide! But they had paid for the work in hope of commercial profit, and they weren't about to let anyone else have the data.

There are parts of the government that act that way, too. The thesis is that since the government has paid for the work, then the government is not going to give it away. The arguments can become quite tangled, but to me it is a form of classification. There are great similarities between security classification, this sort of classification, and the company proprietary sort of classification. The argument that has to be carried on in the patents and copyrights section, and among the makers of policy for government ownership of infor-

mation is what is the government going to do with the information, once it has it? What is the purpose of having it? Why did the government sponsor the work that produced the information?

My general answer is that the government sponsored the work because it needed to be done and no one else was doing it. But we are not going to get the benefit of the work unless we can get the information to someone who can use it. Being possessive about the information is going to get in the way of the basic reason why the government stimulated the work in the first place. The arguments are complex, and the answers are often not very clear. The problems appear in all of the services, and the decisions are very like classification decisions. Thus, I think some of you may from time to time become involved in cases of this sort.

There is in all of the services another special case that intrigues me for classification reasons: the subject of environmental information. The Navy sponsors a lot of work in oceanography because it needs the detailed data about that environment. The Air Force needs meteorology, and the Army needs information about climate and geography. These are data that most people tend to think of as unclassified. But it is not so simple. There were running arguments in the Law of the Sea negotiations for a long time about whether there was a difference between oceanography and military oceanography. There was worry about the availability of all those classified data. I can only say that data are exactly the same, whether they are sponsored by the military or sponsored by the National Science Foundation or NOAA. It is the intended use, or the fact that we intend to use the data, the correlation with application, the layout and translation into forms that can be used by military operators that may turn out to be classified. The data, themselves, are pretty well unclassified. There may be a valid argument for protecting the fact that the Navy wants particular data on selected parts of the world's oceans, but we have to be very careful about how we impose the security restrictions.

There are problems, for instance, with technical data acquired from classified platforms. Some very good scientific work can be done with satellites, and very good work can be done with submarines. We have occasionally found ourselves in trouble with publishing submarine-derived data because the scientific community won't accept them unless it is clear how the data were obtained. In fact, one must provide all the *details* of how the data were acquired, because that is how science operates. But an explanantion of just how the data were taken would explain something about a military capability. We were really at an impasse. We had good data, but we couldn't get it out to the community which needed it and thereby get the best return on our investment in the whole operation. The actual use of that completely basic data, quite aside from any operational interpretations, was badly restricted because of classification problems.

The last real problem I want to talk about centers on the related field: how do you handle much of the satellite data, which are often of excellent quality. There are serious arguments about the extent to which we can use the full range of available sensor capability for generally civilian operations. There are still arguments about the significance of saying something about the resolution of certain sensors, and those arguments go on until the next incident where a vendor has managed to get a picture of the West Coast, say, taken with his sensor, published in a nice national magazine. Either no one really thought about the significance of that picture and what it would reveal, or in fact someone wanted to publicize the capability. Most of us, who aren't actively engaged in that particular sort of decision will never know which was the reason; we can only see that something strange happened.

The last point is simply meant to emphasize the original point, that most scientific data need to be published. Operational significance generally, but not always, needs to be protected. How you achieve the operational capability in actual practice almost always needs to be protected, but just as with the sensors you may want the opposition to know what the capability is. If you do tell him exactly how you did it, you will lose whatever lead time you might have been able to generate.

I think that is enough of a general statement on what areas are obviously going to be important to the Navy, and what I think are some of the problems that will face all of us in determining classification now and in the future.

AIR, SPACE & SUPERIORITY

Dr. Bernard A. Kulp
Chief Scientist
Director of Technology,
Air Force Systems Command

I appreciate this opportunity to share some of my thoughts with you on why we feel some things should be classified or protected and what we feel should be protected. Considering our present and projected systems inventory we note that they are becoming extremely efficient in performing their particular role. However, at the same time, their complexity or sophistication is ever increasing. The enemy is devoting significant resources to learning about and countering our systems.

We then are caught in a quandary on what technology to protect and what technology to release to

the public, in order to attain and maintain superiority. In general, we classify only a small portion of the data relating to our systems. This is so for several reasons. First, it costs too much to unnecessarily classify everything. Therefore, we must make a valid assessment as to what the key factors are in a system and then what portions need to be protected.

Second, a balancing consideration is our desire for wide distribution of technical information within our industrial and academic communities. This acts as a catalyst to further developments and new innovative approaches to our problems. Keep in mind, however, that we are giving the Soviets the same data at the same time.

I've already inferred that what I am going to cover is new systems and technology. I will not be covering tactics, operational plans, and other areas normally associated with our unified commands. Further, although the Foreign Technology Division is part of AFSC I will be covering areas related to intelligence gathering or analyzing operations.

I encourage discussion and invite questions about any areas I plan to cover, or those controlled by AFSC which I might not, because of time, address. One caution: we must remember that my comments are unclassified and cleared for public release. Any questions or discussions which result must be kept unclassified as I'm sure all of *you* all understand.

To provide some order to the review, I have chosen to group the systems which I will use for illustration of some point, into five areas:

- Aircraft
- Strategic missiles
- Armament programs
- New weapons

The aircraft area – the largest, of course, is divided into seven categories as shown in Table 1. Each includes further refinements for clarity. To be certain that we are on the same "wavelength" may I define what we include in the various categories.

Program Schedules – Contractor/subcontractor identification, the contract number, model and/or type designator, material priorities, and, as well, information on funding, procurement and production.

Systems – This is the entire aircraft as a whole and covers specifications, performance, physical characteristics, survivability/vulnerability, reliability/maintainability, and signature characteristics.

Propulsion – Would include design, specific performance/operating characteristics, infrared suppression, test data, and fuel capacity.

Avionics – Includes radars, identification friend or foe equipment, electronic warfare items (both counter measures and counter-countermeasures), weapon delivery systems, and voice communication.

Armament – Covers munitions such as missiles or guns.

System Development Testing – Describes the objectives, flight testing, wind tunnel testing and ground/in-plant testing.

Deployment Data – Is the final; it is the concept of weapon system employment, initial operational capability (IOC) and/or desired operationally ready (OR) dates and locations, programmed or projected total force requirements by wing/squadron, unit location, or dates, and "beddown" locations.

In discussing the other major areas we will try to use similar categories. There are, as many of you know, security classification guides for the B-1, F-15, F-16, and the A-10. When you examine them you would note marked similarities among them. Differences naturally relate to specific equipments being described – engines, electronics, armament, *etc.* For aircraft, most information classifications fall into two time groups. The first group is classified for a short period of time, *i.e.*, 3-5 years or through development testing. The second group is classified for an extended period *i.e.*, greater than 10 years, or essentially through the operating life of the aircraft system.

The reason why this difference exists relates to the kind of advantage access to the information would provide an enemy and is in consonance with criteria published by the DoD. For example, in the area of what you might term the airframe systems – empty weight, basic weight, operating weight and fuel capacity – the B-1 is classified only through 1978. On the other hand, the *signature* characteristics (radar cross section and engine plume/IR Signature) are classified through 1987. For the propulsion system for the F-15 and F-16 (F-100-PW-100), reduced test data also is classified only until 1978. However, in the category of avionics, all the classified information on the IFF system for the A-10 is classified through 2002 (and that's similar to the treatment of the IFF system in other craft) while the majority of the classified information on the Fire Control/Weapons Delivery System will be unclassified after 1978. So, you see, even within the major categories that I described there can be differences as to time-requirements for protection.

TABLE 1

AIRCRAFT

	B-1	P-15	F-16	A-10
Program Schedule	U	U	U	U
Systems	U/S	U/S	U/S	U/S
Propulsion	U/S	U/S	U/S	U/S
Avionics	U/S	U/S	U/S	U/S
Armament	U/C	U/C	U/S	U/C
System Development Testing	U/C	U/S	U/S	U/C
Deployment Data	U/S	U/C	U/C	U/C

It can be said that we only classify these items in the long term which if divulged would seriously degrade our effectiveness in a conflict, or provide information an enemy could use to develop a weapon system to take advantage of an inherent limitation or vulnerability revealed by the declassified and released information.

Moving now to strategic missilery, consider our current Minuteman force and the advanced ICBM technology (MX) program. Marked similarities in *approach* remain as shown in Table 2.

TABLE 2
STRATEGIC MISSILES

(ICBMs)

	MINUTEMAN	M-X
Reentry System	S	S
Propulsion	U/S	C
Guidance	C/TS	C/TS
Survivability/Vulnerability	U/TS	U/TS
Funding	U/S	U/C
Basing	U	U/TS

Because of their importance in the Triad we protect more information and technology than we would do in the development of an aircraft system. In fact, ERDA actually provides the classification guidelines for the reentry system since Restricted Data determinations relating to warheads are dictated by public law in the Atomic Energy Act of 1954. There are, besides the warhead, two key areas in both systems. They are guidance and propulsion. In the guidance systems we must protect both the design methodology and systems performance. Similarly, in the propulsion area we must protect the design methodology and actual systems operations and performance. In both areas failure to do so can compromise data relative to the system's total capabilities as well as provide data to the enemy which would reduce its survivability. Basing is one of the few areas where we currently see a difference in what is classified. Minuteman is a hard silo *operational* system and thus silo locations are unclassified. On the other hand, MX is a technology program and the *detailed* data about its basing options would provide information as to projected design and this must be protected. As you may have read, an option under consideration is mobile launch capability. If that becomes operational the location of the missiles at any time will also need to be protected to enable it to survive.

Protecting technology in the area of munitions or armament development can be the key to any future armed conflict. I will cover now several areas on which we are currently working – they are shown in table 3.

The Hard Structures Munition program has been in progress for over ten years and has demonstrated a successful warhead in the last year after an expenditure of approximately 8 million dollars. The warhead is a technical breakthrough in the sense that by the technique used, a large amount of explosive can be buried in solid concrete structures or stone structures and made to detonate with catastrophic effect. If a foreign country decides to attain the same technology, they know that unless they determine *a priori* how we

TABLE 3

ARMAMENT PROGRAMS

	Hard Structure Munition	Laser Guided Bomb III	Improved 20mm/ Ammunition	GAU-8A Gun and Ammunition	Millimeter Wave Contrast Seeker	Radiometric Area Correlator
Program/Schedule	U	U	U	U	U	U
Subsystems						
Warhead	C	U	U	U	N/A	N/A
Seeker/Sensor	C	C	N/A	N/A	C	C
Processor	C	C	N/A	N/A	C	C
Propulsion	N/A	N/A	U	U	N/A	N/A
Performance	S	C	C/U	C/U	S	S
Test Results	S/U	S/U	C/U	C/U	S/U	S/U
Cost	U	U	U	U	U	U

solved the technical problems, they can also expect to expend over $10 M. If the technical approach is known, the cost should be below $2 M.

If the unclassified literature would make it possible to determine:

- the cost of the program,
- that the warhead is for large concrete targets,
- the two events that are involved with the functioning, and
- the size of the warhead.

The average warhead designer could sketch the warhead with little more than that being known and could define a program leading to the successful demonstration of the warhead. With that knowledge, a foreign country probably could develop the warhead at one fifth its cost to us. Then turning to the Laser Guided Bomb (LGB). It was developed during the period 1961 - 1967 from the time the laser was demonstrated until the LGB was dropped in Vietnam. This weapon must have been a surprise to the enemy because of the short time between demonstration of feasibility and the first drops in combat. This is also borne out by the lack of countermeasures in the field.

The LGB warhead is a standard general purpose bomb thus the only classified portions of the program are in the seeker/sensor, processor, and performance and test results. The reasons for protecting seeker/sensor and processor are to assure the highest degree of ECM immunity. Performance requirements and test results are protected to make it more difficult for the enemy to assess our combat effectiveness.

Of greatest importance in each of these cases is to assure that no foreign country realizes a windfall as a result of our release of information, either critical to the development of a competitive system for the world market or providing the ability to counter our weapons in combat.

In the area of gun development, two different types of programs are shown. The 20mm improvement program is upgrading a 20-year old general purpose gun system. The 30mm GAU-8/A program is a developing new system specifically designed for the A-10 aircraft. The only classified information in these programs is the performance requirements/test results. Data on these items have been released in unclassified form for

the purposes of program information and for foreign military sales. Other than compromising our combat effectiveness to an enemy, there is little to worry about since the technologies and production methods are well known throughout the world.

The Millimeter Wave Contrast Guidance (MWCG) program and the Radiometric Area Correlator (RAC) Guidance programs represent the most advanced technologies in our weapons programs. These guidance systems are for all weather/day-night use and if successfully developed into systems, could drastically change methods in tactical warfare. For this reason, extreme care is taken (a) to preserve the U.S. world wide lead in this major area of military technology and (b) to assure maximum protection from ECM.

The world already knows that we are working in the millimeter wavelengths for guidance on our tactical weapons. The world knows that approximately half of our advanced development budget is going into such efforts. The enemy knows that our primary concern is in the massed armored attack. Add to this the knowledge of the windows for transmission in air, the knowledge of target characteristics at these wavelengths and some knowledge of signal processing techniques which the enemy undoubtedly has and nothing is left for him to do but the circuit design and testing.

Thus, one can say that at the very least the arms producer in a foreign country and the enemy start in competition with us with an advantage of knowing our cost and generally what the approach is. If technical details are provided, the technically competent country can beat our schedule and cost.

Now let's turn to a difficult area of high technology such as high energy lasers, shown in Table 4 along with others I shall compare.

In the case of high energy lasers the policy to be applied in classification of technology effort must balance the needs of security for national defense against the need for openness to encourage technical interchange with the scientific community. This is an extremely important need in new and emerging technology areas where the scientific community is generally the inventor and can provide much insight. For this basic reason the physical concepts of the technological approach are frequently unclassified or classified at the lowest possible level while the performance specifications, applications, and effectiveness are frequently classified at a much higher level. For these examples, the level of classification is established by guidance to protect the most critical factors revealing technology goals or maturity. These items must be protected to prevent the exploitation of counter technologies by a potential adversary. Further, the establishment of technological goals tends to indicate program direction and intent.

In a similar manner the schedule or status type information also indicates the goals and direction as well as the technology levels achieved. Potential applications must also be protected in order to eliminate the certainty of approach. If one can acquire knowledge about the potential applications of the adversary's new development, then the difficulty of countering that technology development is considerably lessened. Such information highlights the attractive applications and, by indirection, would help

TABLE 4

NEW WEAPONS

	HIGH ENERGY LASERS	NUCLEAR WEAPONS	ADVANCED WEAPONS CONCEPTS
Performance Characteristics	C/S	C/TS	U/TS
Effectiveness	C/S	C/TS	U/TS
Physical Principles	U/S	U/TS	U/TS
Engineering Data	U/S	C/TS	U/TS
Potential Applications	S/TS	S/TS	U/TS
Status/Schedules	C/S	C/TS	U/TS
Achilles' Heel	C/TS	C/TS	U/TS

an adversary in his screening process and technology development without his investment of resources by eliminating those items which have marginal return. The other critical point is the Achilles' heel, or the countermeasure, of a given technology must be kept classified. In any case of technological advances, protection against providing a potential enemy the knowledge of how to counter them without his having to do the research is of paramount concern.

On the other hand, nuclear weapons are well developed and the principle of creating a super critical mass is known to nearly every high school physics student. The items which must be protected, however, are the details of how the devices are engineered and constructed. The detailed engineering data could be used by some one, such as a terrorist group, to make a relatively crude copy of a sophisticated weapon with "acquired" material. Then the details of yield and fuzing characteristics and consequently effectiveness must also be classified since exploitation of these data by an adversary could lead to increased survivability by selective hardening of sites or facilities that the adversary feels are targets. Finally, the vulnerability of these weapons to any enemy action must also be classified to insure that the maximum effectiveness is not compromised, and that a relatively cheap (in research cost) program can not render our weapons useless.

In the areas of advanced concepts the dichotomy of scientific progress and national security, as I mentioned when discussing lasers, is even more pronounced. While it takes 5 to 10 years to make a relatively mature technology a weapon system, it takes about twice that time to take an emerging technology to fruition. Security in the early phases is critical to maintain the technological edge.

The level of classification in this area tends to be driven by the sensitivity of the potential *applications.* Desired performance projections are often undefined and only speculative within the scientific community until the basic research experiments have been accomplished. Often schedules and detailed status estimates do not even exist, and it is clearly too early to establish an engineering data base.

Here classification levels must depend on the judgement of the classifying authority and the perception of the criticality of technology under development.

Questions & Answers

Question: Could you comment upon your approach or your department's approach on technology intentionally or accidentally released through aviation leaks. I am not being facetious. I am wondering what do you look at.

Answer: Well, we recognize the problem, if you want to call it that, because of the open literature in this country. However, you will note that I did not talk about a number of different aircraft systems. My advance concepts in the last table might well reference a recent *Aviation Week* article on a certain capability. Essentially, the Air Force chooses not to comment. We neither confirm nor deny that we know about a given system, that we are working on it, or that we agree or disagree with anything that is said about it. I think that is probably the best I can explain the Air Force's position in such a situation.

Question: You mentioned new systems. Do you leave it up to the judgment of the classifying authority as to how the system should be protected? If that is the way you are operating, what is the possibility that each authority classifying a different piece of the system effectively results in having the whole system unclassified?

Answer: I think I used the word, concepts and technology in this kind of situation. That is, I used that remark particularly with reference to these very advanced weapons concepts. When we get into a system like the Maverick, there is a very specific classification guide that details pretty well everything in that system that is classified, down to where the nuts and bolts are. So when we have gotten to the point where we are in fact developing a system, we have a systems project office, then a classification guide is developed, and the Air Force agreed-upon classification guides are put out.

In the case of the laser – the airborne laser laboratory – that is now enough of a system so that we have a single office responsible for the classification of all the sub-components. Like the pointing and tracking; like the system design; like the optics involved; like the acquisition system and the handoff. However, in some of the advanced systems, some of the advanced concepts that, for example, the Office of Scientific Research (OSR) is working on, there are many different facets to it – such as the basic research measurements that are being made. Even the machinery that is being designed to make these measurements does run the risk of having somewhat of a disjointed classification approach. It is not really clear to me that it is often over-classified, although again I find it difficult, like many other people, to classify fundamental physical data. However, sometimes the ability to gather certain data represents a capability we would like not to be known.

So in general such cases are at a systems command headquarters or at a headquarters level, like an OSR level, where there are classifying authorities and we don't really get too great a dichotomy of now having the things unclassified or having a hodgepodge of classification in which the most critical element turns out

to be unclassified. I haven't seen that happen in the Air Force weapons concept. Somehow the concept of management where we have a man at headquarters, either systems headquarters or Air Force headquarters, who is cognizant of the total program, has avoided that problem so far.

Question: Have you or your scientific advisors, or the scientific community ever been "pulsed" by the Office of Industrial Security, Department of Defense, for advice and guidance as relating to the time saved reducing the classification periods?

Answer: Yes, certainly we have; as much on declassification as on the release of technology; and I will use a specific example. The F-100 engine. The Air Force believes that the state of the art in combusters in this country is ahead of that of the world. Although the combusters as such, are not classified, again because of the time phasing – they are through development, they are in production – the Air Force recently took a position that we should not release the design and production details of this particular part of the engine to the world. Our technical community was the one that made the assessment that *now* was the wrong time. Three to five years down the line would be a more reasonable time at which we might expect English or French to be at least approaching in such technology. Then would be a proper time to declassify or release.

The judgment of the Air Force technical community was that it was declassified too early and released too early. As you know the Air Force administrative community takes its orders, and I believe the system was released.

A VIEW TO THE FUTURE

Dr. James B. Rhoads
Archivist of the United States and Acting Chairman of the Interagency Classification Review Committee

I appreciate the opportunity to appear once again before this audience of security professionals. The scope of your Thirteenth Annual Seminar is impressive by any standard – as is the array of speakers.

In my invitation to speak I was pointedly asked to refrain from talking about the details of the Annual Progress Report of the Interagency Classification Review Committee. Consequently, just let me say that the report is now being printed and we anticipate that it will be released by the White House around the end of this month. If you are interested in obtaining a copy, please get in touch with the ICRC staff and give them your mailing address. For today's presentation it was suggested that I talk about the future – to present a sort of prognostic report. So, in the next few minutes, I hope to provide some ideas which will perhaps help you view our program goals from a fresh point.

All of you realize that the terms secrecy and disclosure are not part of the Constitution. The maintenance of official records, derived from the housekeeping functions of Government, has been extended over the years to embrace the secrecy of records. The information security system was established by executive action, and, like an exotic mold, just grew – particularly with World War II and in the years following the Korean War. A series of events and executive orders which followed resulted in Executive Order 11652. In April 1973, I became Acting Chairman of the Interagency Classification Review Committee (ICRC), established by the Order, and during the past four years, I have served my apprenticeship in the field of information security.

As a background to the future, I must give you a frank appraisal of the present information security system and Departmental and ICRC implementation of that system from my point of view; both its good points and bad points. I emphasize that this is my own evaluation and does not necessarily reflect the opinions of the members of the Committee.

Let me begin on a positive note with some of the good points about Executive Order 11652:

- It established Government policy which limited classification duration and provided greater public access to the operations and actions of Government. Specifically, it established a system by which a member of the public could seek declassification of particular information or make a complaint about the system – and carry his case to the highest levels of Government without recourse to Judicial action. It also established a system whereby, theoretically, most classified information could be reviewed for declassification after 10 years and all classified information *had* to be systematically reviewed for declassification after 30 years.

- It provided for a drastic reduction in the number of officials who have the authority to classify information. Better control has resulted.

- Finally, it established a system for oversight by a relatively independent body.

With these innovations, the agencies and the Committee have, together, made considerable progress in attaining a coherent information security system with a fair degree of public credibility.

But there are some aspects of Executive Order 11652 which have tended to limit progress. For example:

- Although the ICRC was established to assist the National Security Council in monitoring implementation of the Order, there have never been clear lines of responsibility and authority in this respect. And, on occasion, there have been differences of opinion between the Committee and the NSC staff over fundamental issues.

- Decision by committee is not always efficient, particularly when members of the Committee have very definite vested interests. That is not a reflection on Committee members, it's just the nature of committees.

- Although the Committee is established as a permanent body, it has no clear place in any organizational structure. This definitely colors the light by which various Departments view its authority.

- The Order is quite permissive in some of its language, using the terms "Wherever possible" instead of "shall" or "will." Therefore, compliance with certain provisions is, in effect, voluntary on the part of the Departments.

- There is a need for a more viable enforcement mechanism to be built into the Order with respect to compliance.

- The system for controlling the duration of classification, that is, the general declassification schedule and the four exemption categories, in many cases inadvertently forces material into a period of continued protection that is not warranted and may not have been intended.

- The system is too complicated and difficult to explain, especially to those who have no background in security matters.

Coupled with problems inherent in the Executive Order are problems inherent in the rapidly increasing rate of change in our modern, technically oriented society, all of which suggest the need for some drastic changes in our program.

First, on the inexorably rapid increase in new knowledge or new "information," if you will. Toffler, in *Future Shock*[1] says:

> "Today change is so swift and relentless in the techno-societies that yesterday's truths suddenly become today's fictions, and the most highly skilled and intelligent members of society admit difficulty in keeping up with the deluge of new knowledge – even in extremely narrow fields."

And then, Dr. Robert Hillard, of the Federal Communications Commission, points out:

> "At the rate which knowledge is growing, by the time the child born today graduates from college, the amount of knowledge in the world will be four times as great. By the time that same child is fifty years old, it will be thirty two times as great, and 97 percent of everything known in the world will have been learned since the time he was born."

Granted, the definition of "knowledge" is vague, but there can be no question as to the rising tide of new knowledge and its concomitant impact on any information security system.

As I see it, the provisions of the current Order are geared to deal primarily with information recorded on a finite number of sheets of paper. The requirements for marking, record keeping, transmission, and declassification cannot so readily cope with masses of information recorded on microfilm, presented visually, or in machine readable form; despite the existing provisions of directives.

Second a factor which has been more in the forefront lately – as you are no doubt aware – is that we are in an era of openness in Government – a firm policy; and an understandable course in the aftermath of the last decade. Now, openness doesn't mean wholesale revelation of secrets, however they are defined: it means judicious decisions to determine if the public good is best served by disclosing or withholding information. The current Order does not provide sufficient guidance, nor an easy, responsive system for making such decisions.

There *are* some additional factors which we who are charged with the oversight of the security program should consider in planning any system for the future. They are not driving forces, but are more in the nature of "lessons learned" from past experience. Let me mention them briefly.

First, there is a great need to simplify the entire system. Especially needed is simplification of marking requirements. Simplification has many advantages; in addition to saving time for the security manager. It can cut costs drastically. It can reduce time spent in security education and training. It will result, in the long run, in better compliance because people tend to follow rules they readily understand. And, of course,

---

[1]Toffler, Alvin, *Future Shock*, Random House, New York, 1970.

simplification will permit a much greater degree of standardization in procedure among Departments.

Second, we need to break the linking of classification level with the duration of time protection is required. Some indications exist that a higher classification level than appropriate was assigned to information because it needed protection for eight years, say, rather than six under the specifications of the General Declassification Schedule.

Third, we need to concern ourselves more with the area of personnel security. A tremendous share of our dwindling security resources is used in this area. There appears to be a need for standardization of processing and a system of reciprocity with respect to accepting the results of investigations among agencies. There has to be more efficient and more cost effective ways to evaluate personnel from the standpoint of security.

Fourth, we need to give further consideration to the development of a policy which establishes more stringent sanctions for those who abuse the classification system. As presently written, the Order only provides for sanctions for repeated abuse through unnecessary classification or overclassification. Similarly, additional study and consideration should be given to the development of viable deterrents which would further limit the unauthorized disclosure of classified information.

Finally. Oversight should extend beyond the major agencies in the Washington area to the field and to Government contractors.

All these factors that I have mentioned, and many more, require consideration in planning toward an information security system for the future.

As most of you are aware, the ICRC staff initiated an intensive program of on-site reviews and inspections of Departmental programs during the latter part of Calendar Year 1976. During that year, over 50 such detailed reviews were conducted. Over 200 are scheduled for 1977. These reviews have been most effective in assisting the Committee in fulfilling its oversight responsibility and in identifying problem areas which require continued Committee oversight. Based on the results of such visits, there appear to be several areas which I personally feel should be addressed in any future changes to the present information security system.

- For example, I would hope that any future system adopted would place greater emphasis on earlier declassification of offical information.
- I would like to see a clear separation between the degree of physical protection required for material and the duration of that protection.
- Most certainly, any future system should be constructed to simplify the system -- particularly marking requirements.
- I feel very strongly that mandatory paragraph marking should be part of any future system. This will contribute to greater consistency in classification and will most certainly facilitate the review of documents requested under the provisions of the Freedom of Information Act, as amended, the Privacy Act, or the Executive Order.
- I feel that, to the maximum extent possible, future systems should be consistent with the provisions of the Freedom of Information Act, as amended.
- Finally, I would hope that future systems will provide for a more independent oversight body with greater responsibility and authority.

I have just given you some very candid personal views on the future. How can you of the National Classification Management Society prepare for the future? The key is perspective and flexibility. We must keep firmly in mind that classsification management is only one of many activities which contribute to the successful accomplishment of the mission of protecting the Nation's security. We must always be aware that security can never be absolute and that there are times when considerations other than security must be paramount. The discussions planned and being held at this Seminar make it evident that you have the perspective and flexibility to help steer the information security program into a brighter future.

Questions and Discussion

Question: Dr. Rhoads, there's a great body of information which is identified in the Freedom of Information Act as being properly withheld from public release other than that which is classified. However, how do you identify that information as not being available for public release? How do you identify it in terms of safeguarding? That's kind of a rhetorical question. My question really to you is should not those categories of information be identified in an executive order of some fashion so that the internal security of the United States is protected as well?

Answer: That's an interesting question. I suppose that it certainly would simplify the review of material that is being requested under the Freedom of Informa-

tion Act if there were some system of identification of that kind. But it occurs to me that with the exception of material which is security classified, the other categories of material which may be exempted from disclosure under the FOIA are permissive and not mandatory categories. I wonder whether, if you had some kind of a marking system of this kind, the tendency might not be to over-withhold rather than to judge each of these categories of possibly exempted material on their own merits in individual cases. That's just a very preliminary thought and is not based on any great amount of consideration.

Question: Further in that connection the Department of Defense at least has authorized use of the term "For Official Use Only" for certain categories of information but this is not true necessarily in other departments. On the other hand, an atmosphere has been created since the Freedom of Information Act -- I think created ourselves -- that we have enough trouble with people who are passing out classified information that is stamped; without a stamp of some kind there's the atmosphere created that such information belongs to the public; and that's not necessarily true.

So the real question is, should we not address this facet in some fashion?

Answer: Well, I certainly do think, and I mentioned this in my talk, that to the extent possible in developing any revised executive order or in the event that the Congress should legislate on this matter, that a major part of the effort should be to make sure that whatever we come up with fits well with the Freedom of Information Act and tracks it as closely as possible and provides for a well integrated system as between the two pieces of legislation.

Question: I would like to know if you have been approached by any representatives of Congress or anyone else to obtain views, your views, on the information security program. I think most of us feel that your views are very close to our views.

Answer: I have not recently. In years past, I have testified on The Hill on bills that have been introduced to alter or to revise and make statutory the classification and declassification program. I think that based on past experience that I'm likely to be approached and asked for my views when serious efforts are underway to alter the system. That's been my experience up to now. But just recently, I have not been called upon.

Question: Dr. Rhoads, as a defense contractor we receive classified material. Frequently included in the same package are items marked "For Official Use Only." Doesn't this conflict with the defense industrial security program? If so, what are industry's responsibilities relative to the protection of this?

Answer: I don't think it conflicts with the executive order and it seems to me that questions you may have on that would be best taken up with the agency for which you serve as a contractor. I think that would be the best.

Question: Wouldn't the caveat "For Official Use Only" be used to delineate material which falls within the Freedom of Information Act?

Answer: Not necessarily. It might, but I don't think you can assume that across the board. Again, I'm not all that familiar with just what classes of information the various agencies may include within the "Official Use Only" category. So I'm not your best authority on that.

Question: Dr. Rhoads, several times you mentioned marking changes. Has your committee studied this very closely? What recommendations would you make for marking changes?

Answer: I don't have any specific recommendations to make on marking changes. I just have a feeling that this process could be simplified without detriment to the program and that it's one thing that any group studying a revision of the system ought to address. The ICRC I don't think has ever really given that any extended consideration. I am hopeful that any efforts within the executive branch to take a fresh look at it will do so, but I wouldn't want at this point to come down hard in favor of any particular change.

Question: Do you believe that the current Executive Order 11652 provides authorization to classify material provided to us by foreign nations which does not meet our classification criteria and which that country has not classified?

Answer: My off-the-top-of-the-head reaction is that there is no basis for our classifying such information. I think if you change the scenario just a little bit and say that it's something that may not meet our standards for classification but has been classified and is demanded to be kept classified by a foreign power, then we're in a somewhat different situation. And I'm not comfortable with that situation. However, there you open up a lot of sensitive problems. I think there's a lot of that kind of material around.

Question: We in DoD and the State Department, I think face this problem. There is material foreign nations do not want released under the Freedom of Information Act here, but yet they don't consider it classified.

Answer: I don't think they ought to be able to have it both ways.

Question: I was interested -- in view of the committee's five years of oversight experience -- in what your views are regarding whether the services have overused the exemption authority for classified information as opposed to following the General Declassification Schedule (GDS).

Answer: I have sort of a gut feeling that probably there has been more of that than there needs to be but I can't prove it. Certainly one of the things that the committee is concerned about and has interested itself in increasingly is to reduce the amount of material that's exempted from the GDS. I think that's a fruitful area for it to pursue. I wouldn't say that there's been flagrant abuse, but sometimes it's a lot easier to exempt information than to do the hard thinking that's implied in handling it in another way.

Question: Dr. Rhoads, you talked about some of the future changes that you'd like to see. Just how far are we down the road perhaps in the new administration to the issuance of a revised or a new executive order?

Answer: The new administration began showing a fair amount of interest in this early on. And I guess that was forecast by some of Mr. Carter's campaign pronouncements. Plans are underway to establish a working group. I'm not sure yet just what its membership will be, but I expect it to meet very soon to begin the work of reviewing the existing executive order and developing a new one based, I would hope, in part or at least taking advantage of the work that was done in the previous administration. It did get fairly far along on a similar effort. I would think that probably the outcome in this administration would be somewhat different than it would have been had that been pushed to completion in the previous administration. But certainly a lot of the work that the earlier committee did is going to be of some value.

I wouldn't be surprised if sometime this fall we had a new executive order, but that's just an educated guess.

PROTECTION AND FOREIGN DISCLOSURE – A CASE FOR BALANCING

Mr. Joseph J. Liebling
Deputy Assistant Secretary of Defense (Security Policy)

I always enjoy appearing before this society's membership, particularly in a forum like this because it provides an excellent opportunity to exchange views that ultimately benefit all of us.

I'm sure you recognize that we are living in an era of changing values. Energy crises and economic stresses call for re-evaluation of our worldwide national priorities. The United States' formidable national defense posture in the world today is due in a large measure to the dominant techological and scientific position which we have enjoyed. The Department of Defense, U.S. industry, and the academic community have a sustained record of accomplishment in keeping the United States in the forefront in military technology.

While recognizing the importance of free exchange of information to support advancement and technical progress of the United States and its allies, it must be equally recognized that certain information requires security constraints vis-a-vis adversary nations, if the United States is to maintain its position of superiority in military technology in the interests of national security. The preservation of the U.S. leadership position in military technology is of paramount importance to the U.S. national interest.

I'll make a distinction between national security and national interest because obviously national interest has a much broader scope. And there we deal with, of course, the foreign relations, the political facets, military and also the economic needs of the nation.

It has been contended that our position today is being eroded. With this in mind, I want to discuss the national security implications that concern us all and the export of technology which the United States considers to be a critical national asset and the importance the classification management role plays in safeguarding our technological lead time that is vital to the effectiveness of our defense forces. In this connection, there are certain factors I want to highlight.

First, however, I want to identify technology in its proper context as we in defense view it today. I am sure you recognize that we are not concerned with the great mass of commercial technology that is developed by the United States, the export of which would not impact on our national security. Therefore, in order to determine which technologies we should protect from a strategic or criticality point of view, the Defense Science Board under the aegis of the Office of Defense Research and Engineering, formed a task force in the summer of 1974. In their deliberations, they reviewed all aspects of exports of U.S. technology to determine exactly which technologies are critical to our national defense needs. Their report is entitled *An Analysis of Export Control of U.S. Technology, A DoD Perspective,* together with the recommendations they submitted, (4 February 1976) it has become central to defense thinking on the problem of critical technology transfer.

I might indicate that the report findings are under current review, and there are several groups working on them. I will cover their various recommendations

presenting both the view espousing protection as well as the view espousing release. Remember as I cover them, however, that the government's position has not been finally established.

The Defense Science Board's task force finding that is most significant for our purpose is that design and manufacturing know-how are the principal elements of strategic critical technology that must be controlled. While the task force placed primary emphasis on design and manufacturing know-how and control mechanisms that transfer it to a potential adversary, they also considered that technology contained in applied research and development may be of significance in selected areas. However, it is design and manufacturing know-how that impact on a nation's capability, that which we call "turnkey operations," or a phase which the Board uses, "keystone operations."

One of our government's far-reaching problem areas is technology transfers and strategic trade control involving international exports and trade by United States industry. Technologists and policy managers have the same concerns and interest in any transfer or trade which results in communist countries gaining access to materials, products or processes having direct or potential military applications. Where the criticality emerges is in the high end of the advanced technology spectrum that would permit marked reductions in development or procurement lead times thereby ultimately resulting in strategic or tactical weapons superiority. Foreign access thereto could substantially close any leadership margin we might now enjoy.

The importance of technology as a major national asset in its application to national defense was first recognized during World War II. The post-war transfer of technology was dominated by the requirement for secrecy in one highly specialized field as evidenced by the stringent controls established by the Atomic Energy Act under the monitorship of the former Atomic Energy Commission for the handling of all atomic energy technology. Wartime controls on commercial exports and technology were also extended but were considered a temporary measure intended primarily to deal with inflationary short supply situations arising in the wake of the war. These controls were supervised by the Department of Commerce.

During the Cold War, the United States established more comprehensive policy for the protection of technology important to national security. The result -- the Export Control Act of 1949 -- provided general authority to restrict the export of goods and technology which would make a significant contribution to the military potential of any other nation or nations which would prove detrimental to the national security of the United States. It authorized the use of export controls to further U.S. foreign policy and to protect the domestic economy from the excessive drain of scarce materials and the inflationary impact of foreign demands. The intent of the act was to impose controls on export of strategic materials and technology to communist bloc countries. Unilateral controls were to be backed by multilateral controls administered by NATO through an organization known as COCOM meaning the Consultative Group Coordinating Committee. U.S. participation was placed under the jurisdiction of the Department of Commerce. COCOM is essentially an embargo program and deals with all our NATO allies except Iceland. Japan is the only non-NATO member. Its basic aim is to preserve for its collective membership a five to ten year lead over the communist world in technological equipment, patents and fabrication methods. The most important fields under constant surveillance include electronic and communication components, telecommunications and radio relay systems.

In 1951 the Mutual Defense Assistance Control Act, known as the Battle Act, as amended provided authority to cut off U.S. military and economic assistance to any country transshipping or re-exporting controlled products to communist countries. Treasury regulations in 1953 extended these controls to U.S. citizens and corporations residing abroad. Finally, the Mutual Security Act of 1954, as amended, authorized the State Department to control the export of weapons and related technical data. Today the Export Control Act of 1976 governs.

Notwithstanding these controls and established responsibilities, a draft study entitled *U.S. Technology Policy* undertaken in 1976 at the direction of former Secretary of Commerce Elliott Richardson and issued in March of 1977*, covers the entire spectrum of science and technology and its relationship to the nation's economic welfare. The study highlights the lack of assessment of foreign technology. It states, and I quote, "No government agency is responsible for the continuing assessment of foreign technology developments in non-communists countries. This omission contributes to present export controls inadequately protecting national security and economic interests that involve critical design and manufacturing technology." The study contains as a possible action, the establishment of a policy board for export control, including the international transfer of technology, *per se.*

Now these are some of the points the study brings out. The board would be composed of the President's Science Advisor, a representative of the National

*(Ed. Note: The report referred to is *U.S. Technology Policy*, A Draft Study, Office of the Assistant Secretary of Science and Technology, U.S. Department of Commerce, March 1977. Available from NTIS on number PB-263 806)

Security Council, the Director of Defense Research and Engineering in the Department of Defense, the Assistant Secretary of Commerce for Science and Technology, the Assistant Secretary of State for Oceans and International Environmental and Scientific Affairs, the Deputy Administrator of the Energy Research and Development Administration, the Deputy Administrator of NASA, and the National Intelligence Officer for Economics of the Central Intelligence Agency, from among whom the President, of course, would appoint a chairman. The Board would also establish a working group composed of carefully selected individuals from the government and private sectors who would aid in developing positions on a broad policy basis.

In addition, the Board would establish a set of joint government/industry committees including experts encompassing all the technologies in the three major areas of export concern -- military products, nuclear power, and commerical technology. These committees would provide specific scientific and technical advice to the policy board regarding the products requiring validated licenses. The Board would further establish the technological guidelines for use by the agencies responsible in administering the controls. All current existing Department of Defense and Department of Commerce committees, whose functions would be replaced by this single interagency board with its coordinated set of government/industry advisory committees, would be abolished.

This proposal has been widely circulated in governtogether top government officials and industry technicians. Industry, as far as we're concerned, has an extremely important role to play.

I would like to address specifically three categories of exports that should receive primary emphasis in our control efforts. Classification management and industrial security specialists play a vital part in the control mechanism through your efforts to meet the rapidly changing requirements of the times.

The first category of exports that should receive primary emphasis in control efforts as determined by the combined group of industry and government specialists is "arrays of design and manufacturing information that include detailed how-to 'instructions'," This category covers exports of arrays of design and manufacturing information plus significant teaching assistance. It has been stated that the export of this kind of information will provide a technical capability to design, optimize and produce a broad spectrum of products in a given field and, therefore, this is the highest and most effective level of technology export. It will provide a basis on which the recipient nation can build further advances in technology.

The next category involves the export of manufacturing equipment. In this connection, "keystone" equipment or "turnkey operations," as I referred to it earlier, has the most important strategic significance which stems from its uniqueness. If the unique equipment is the only equipment differing from remaining general or multipurpose equipment, its uniqueness is evident and should be protected.

The third category involves products with technological know-how supplied in the form of extensive operating information, application information, or sophisticated maintenance procedures. Elements of design or manufacturing know-how are embodied in this type of information. It is often included in sales of such complex high technology products as electronic computers.

The task today in government and industry is to refine and mold a program that can better accommodate national security, be practical, safeguard our critical technology, and be responsive to industry and their export requirements so vital in the interests of promoting international trade.

One method is weapon systems classification where essential for national security reasons. It is an effective mechanism for controlling the critical technologies embodied in military systems because the knowledge is usually limited to those people whose efforts are governed by a contract with a user agency that, by reference, incorporates the safeguards under the current procedures and policy requirements to which a contractor is bound, by contract, under the Department of Defense Industrial Security Program.

Another facet is completely the opposite side of the coin, as I indicated earlier. While we talk about constraints and withholding vital technology, there is a dilemma brought about in government today by policy makers and decision makers and by those who have to adjudicate an individual case as to the balance principle involved. Along these lines, is a facet which suggests that there is a competing view in the unequivocal need to remove security classification as rapidly as possible, when conditions permit, through the life continuum of weapons technology.

For many years I have advocated – and this is the current Department of Defense policy – downgrading and declassification programs on a progressive time-phased basis. It is my view that through that policy we derive real benefit from the following factors.

- Improving the flow of information to the news media and the public regarding current defense posture;
- Increasing the industrial base because of availability of such information to small business;

- Facilitating international trade and export by American industry;
- Permiting a wider exchange of know-how among the scientific and technical communities including colleges and universities – domestic and international;
- Providing for the availability of current state-of-the-art technology for commercial and civilian purposes so vital to the economy of the United States; and,
- Reducing costs associated with safeguarding classified material.

This last point has been instrumental in reducing industrial security costs and has resulted in several million dollars of program cost avoidance and savings.

Notwithstanding these factors, let me go to another point which, again, I indicate is the other side of the coin. It is interesting to note that following World War II, a program was undertaken to declassify millions of documents which could be of advantage to business, science and industry. At that particular time I managed a program for the Air Force, and there are several of you here with whom I worked on this program.

Some of the technology involved at that time included advanced principles of doppler radar, moving target indicators, production processes, operational characteristics of then-current state-of-the-art weapon systems, as well as reports from the wartime Office of Scientific Research and Development and the National Advisory Committee on Aeronautics Research Council. Some of the technologies represented are used today, although they have been updated and product engineered to accommodate our more modern weapons systems. A result of the declassification effort at that particular time, was the remarkable progress made in this country involving the most superior electronic industry in the world. Several years later in the intelligence community it was indicated that the Soviets, relying heavily on this same declassified technical information purchased openly, made great strides in their own field of electronics and countermeasures thereby enhancing their competitive military capability.

Question: Where was the greater benefit gained? I prefer to support the school of thought that the technological and industrial communities in the United States are the real beneficiaries.

As I mentioned, regardless of these factors, what I am saying now is that much of the information considered by the Defense Science Board to be strategic and critical technology may be unclassified, even though it is technology which advances the state of the art or establishes a new art in an area of significant military application in the United States. Nevertheless, this strategic and critical technology requires control. The current administration's interest in controlling nuclear exports and non-proliferation policy is a most significant example of our concern. The United States retains a considerable technological leverage in the intensified bargaining over the proliferation of nuclear weapons exports. This fact was reflected in recent legislation sent to the Congress by the President and resulting in the meetings that are being held in NATO.

In the Department of Defense, we're developing an export policy that defines critical technology as classified or unclassified nuclear or non-nuclear design and production know-how, software, test data associated with weapons and military development programs. This would include technical services and information of any kind that can be used or adapted for use in the design, development, production, manufacture, utilization or reconstruction of implements of war including technical data relating thereto.

The subcommittees – of which there are four established as a result of the special study of the Defense Science Board – are considering, that to preserve strategic U.S. lead-time exports could be approved if they represent only an evolutionary advance. On the other hand, in order to preserve strategic U.S. lead time, exports should be denied if the technology represents what we call a revolutionary advance to the *receiving* nation. Of course this is related to what we call state-of-the art.

Our export policy must maximize lead time. If the receiving country is on the same evolutionary track, the transfer of certain technology may be desirable. If, however, the receiving country would obtain a revolutionary gain, then the transfer must be denied. The object of applying export controls to strategic design and manufacturing know-how is to protect the lead time of the United States as compared to other foreign countries.

We are not talking exclusively of communist bloc countries. We're also talking friendly governments because of what we call the re-export principle and third-country releases. When we supply technology on an offical basis to foreign governments, a great deal of the technology is fused into the wrong developments and the controls on an international basis are very difficult to achieve.

Lead time should be determined by comparing the position of the United States in the technology area against both the receiving country's current manufacturing practices and processes and the velocity of their advance in that technology. Such a determination should be made by individuals from both government and industry involved in the practice of the art supplemented by and relying heavily on the intelligence community.

It must be understood that technological lead time is extremely perishable. It dissipates quickly as the basic concepts and know-how become widely known and exploited. A lagging country can narrow the gap even without benefit of active export transfer mechanisms. This happens because the leading country must work its way up the incremental track without outside help while the lagging country advances both by its own incremental efforts and by the general diffusion of technology to which I just referred. Competitive allied government and third country releases for considered legitimate economic trade also add to the complexity of uniform application of policy affecting enhancement of military capabilities. This is something that's negotiable with foreign governments through NATO, and the other international arenas. Such competition also poses a real problem in critical weapons programs and related technology offered for sale to underdeveloped countries who cannot maintain and support these equipments.

The four major levels of technology transfer are product sales, support, co-production and co-development, and, solely co-production. From a broad defense policy point of view, co-production and co-development or co-production by itself are the most controllable because there is a memorandum of understanding negotiated in each case to definitize all the various elements of agreement which are programs, such as foreign military sales, licensing agreements, normal export control and so forth. There are standard provisions. If it's classified, of course, the national disclosure policy prevails, and these standard conditions and criteria must be met: the protection of the product; the assurance of their people that it will not be transferred further; and that it will only be used for military purposes.

I firmly believe that to be effective classification management specialists in today's diversified decision making environment – and we have discussed this with you at earlier meetings – must use the expertise of the corporate industrial security specialist, the marketing personnel, the system program managers, and the manufacturing specialist. In this connection, I urge you to read the *Industrial Security Letter* which we put out through the Defense Logistics Agency dated 15 April 1977, particularly the lead article which is entitled "Marketing Activities with Communist Countries." It sets forth the latest policy guidance relating to procedures to be followed when dealing with communist countries and any other foreign country involving both classified and unclassified technological information.

In closing, I want to discuss certain significant recommendations submitted by the Defense Science Board Task Force which, as I indicated earlier, are now under consideration by the Department of Defense in liaison with the Departments of State and Commerce that may have certain merit. They recommended that Defense should develop policy objectives and strategies for the control of key high technology fields and that these objectives should include sufficient information to identify key elements of the technology including critical processes and key manufacturing equipment. Technology exchange opportunities should be identified by citing technologies in which the U.S. lags the communist world so that subsequent claims of Quid-pro-quo exchange are not used as a means to circumvent the control of strategic technology.

At this point, let me give you an indication of the comparative status of the U.S. and Soviet technologies which is taken from a statement by Dr. Malcolm Currie, Director of Defense Research and Engineering, to the 94th Congress in February of 1976. I'll go through some of the list for you to indicate the technology today on a comparative basis between the United States and Soviet Union because many of you here, of course, represent corporations who have products in the specific fields.

In the field of high pressure physics, the U.S.S.R. leads. Integrated circuits fabrication, such as microwave semiconductors, the United States leads. In welding the U.S.S.R. leads. Computers, the United States leads. In titanium fabrication, the U.S.S.R. has a strong lead. In high yield nuclear weapons, we're on parity. The U.S.S.R. has made several unique developments currently. In high by-pass ratio turbo fans in the jet engine field, the United States leads. In high frequency radio wave propogation, the Russians appear to have a strong lead in several applied areas. In air-to-air missiles, the United States has a strong lead. In the numerically controlled machine tools....these are unclassified products....the U.S. leads. This is the type of item we're talking about which has been considered in the commercial arena for possible controls.

In the field of avionics, the U.S. has a strong lead in radar for surveillance, bombing, and air-to-air combat. In magneto hydrodynamic power generation, the Russians lead. In composite materials, the United States leads. In aerodynamics, this is mixed. In inertial instrumentation, the United States leads. Antiship missiles, the Russians lead. Chemical warfare, the Russians lead. In precision guided weapons, the United States leads. In satellite-borne sensor technology, the U.S. has strong and increasing lead in areas where comparisons are possible.

That brings up something that you've been reading about in the news media in the past couple of days which I won't address myself to any great degree. That's the possible use of laser beams by the Soviet Union to shoot down satellites. It's the contention of some of our technologist policy makers in this country that we're unaware of this type of development. But the possibilities are there, of course. In the field of

high energy lasers, which is what I referred to in the laser beam attacking satellites, we're uncertain. As Dr. Currie indicates, the Russians have a large program involving approaches not being pursued by the United States.

Now when we talk about the lead of one government versus another, there are to be considered various reasons and factors other than the technological point of view. From a strategy point of view or from a foreign intelligence point of view or from a military capability, one government may put its funds in one particular area while the other concentrates on an entirely different field of interest. Therefore, it's very difficult to get a good basis for comparison. This is why in some of the congressional hearings there is a tremendous amount of controversy as to who really leads in a national defense effort – the U.S. or a communist bloc country.

Some of the other recommendations outlined by the Defense Science Board indicate that we need more communication of policy to interested U.S. agencies, to private firms and to foreign nations. We must obtain a wider base of cooperation in effecting controls, a most difficult field to get at because of the economies of nations involved.

Advisory committees consisting of individuals from government and private sectors should be used to recommend policy objectives and strategies and to update then continuously.

The Task Force also advocates that objectives and strategies for controlling these technologies should be developed by knowledgeable individuals from both government and private sectors. And additionally, that these study groups should identify the critical elements of know-how not previously defined. This is what the groups are doing today. It is a most difficult field because some of these products have technologies that can be used in commercial, non-military, non-defense effort, yet the process or the know-how can be adjusted by a foreign government if it wants to apply it to the military field. The nuclear propulsion field is probably the most significant and the most readily assimilated by anybody professionally oriented in this field.

Furthermore, adequate resources must be allocated to interface with the groups developing this information. We have no means today in the government – we've cut down on personnel and that sort of thing – to provide for implementation of these objectives in technology transfer cases until the results of the studies that I've been describing in this entire presentation are completed. Policies are being drafted now which will go to the highest seats in our government for approval, such as the National Security Council and possibly the President.

The Task Force believes that if the Department of Defense in collaboration with the other interested agencies can accomplish these objectives, it can effectively reduce the time element involved in the case-by-case analysis of export applications which is a lament constantly expressed by American industry. They stressed developing policies for the control of strategic know-how in advance of case-by-case requirements so that U.S. objectives are more clearly defined and broadly understood by U.S. agencies, industrial firms, and other friendly nations.

Introduction to *FROM CONCEPT TO MANUFACTURE*

James J. Bagley
RB Associates
General Chairman

This introduction to what amounts to a substantial portion of our seminar – *your* participation – is merely to set the stage, as it were. We begin with an humorous exercise, for which we are indebted to Frank Larsen and his group in the Office of the Chief of Naval Operations, entitled *The Three Little Pigs*. It is intended to develop a sense of

- What do words mean
- How do they affect interpretation of guidance
- Why is it necessary to be quite specific

Then, we have developed a sequential exercise that will consume all of our available time – one which is quite different from *The Three Little Pigs* mentioned above. The approach has been to postulate specific improvements in an expected tank (*i.e.*, the XM-1) in the context of priorities as viewed by statements of the Chairman of the Joints Chiefs of Staff and the Director of Defense Research and Engineering. The view for attainment of the goals is the 1990s. To make it credible, we have examined the existing system and have concluded that to ensure marked improvement, it is necessary to develop a secure communications system and a target acquisition and designation system with a goal of first round on target at a minimum range of 6 kilometers under all weather conditions. It is emphasized that this exercise was developed with no information on what might actually be underway in the Army; we have not had access to specific tank development information. Your Chairman, as a devotee of Armor and having had some experience as a tanker in the past, concluded that the best way to improve the system was to improve command and control by developing a secure communications system; to be interoperable with foreseeable satellite communications. That improvement combined with a new and improved

acquisition and designation system would result in a *significant* improvement in our land warfare capabilities.

Why was this topic chosen? As commented above, to make it credible we examined the writings and testimony of a recent Secretary of Defense and the Chairman of the Joint Chiefs of Staff on critical needs of the United States. Their feelings were best summed up by a recent Director of Defense Research and Engineering who said:

> *It is in the area of land warfare systems that I am most immediately and urgently concerned. The Soviets in many cases are widely deploying technology now for which we will not have roughly comparable counterparts until the early to mid 1980s.*
>
> Dr. Malcolm Currie

You might recall the words of our speakers in this regard.

As this is a return to the fundamentals, we also decided to have the exercise conform to the current world of determinations; that is, to start the exercise from the development of the requirement at the Departmental Staff level; assign the requirement to a Systems or Material Command for development; have the SysCom select a Prime Contractor; have the Prime Contractor decide what sub systems would be subcontracted; decide what and how much security guidance would be needed by the Sub-Contractor (concurrently deciding what guidance is needed for the total system), and determining what guidance was available as well as what is needed. Finally, the Sub-Contractor would determine how to respond to the Prime Contractor and produce a sub system compatible with the terms of his contract. This, in turn, would become part of the total system.

This then, is the summary of events for the exercise – to develop the security guidance for four separate but interrelated parts, fulfilling a requirement which started from an established need; the assignment of responsibility; the selection of a contractor to do the job; and his selection of a major sub-contractor. The exercise also considers logistics such as depot maintenance and repair, as well as the means to destroy the critical components by a new destruct system. We hope it will be an exercise that will pique your interest, and, for some of you, provide an experience in developing guidance at successive levels from top to bottom.

Obviously, there can be many potential solutions – some will be better than others because of background and experience. For those who work at the Chief of Staff level, it will be an example of the problems faced by the "troops" in trying to figure out what was meant as well as trying to figure out what really is sensitive about the requirement. For the SysCom it would include the process of trying to coordinate the various problems – intelligence, security, contracting, publications, *etc*. For those of you at the Prime Contractor level, it is an attempt to show that requirements do have a basis, although you may consider such less than obvious. Further, it is an attempt to show the need for decision-making at the Prime Contractor level; for example, what will be sub-contracted; and, fitting the guidance needs to the procurement package – which is another way of saying that the sub-contractor has a need for certain guidance, or does not have a need for guidance.

All of the exercise is geared to the new Contract Security Classification Specification, DD Form 254, recently approved for implementation by DoD. *NOTE WELL* This is a new "ball game." At each level of responsibility contracts will be required to have *narrative* guidance. In a word, as NCMS has been "preaching" for many years, classification guidance is the name of the game. Details of the exercises and further explanations are included in Part II of this volume.

THE SUPERCRITICAL WING–A CASE OF UNCLASSIFIED HIGH TECHNOLOGY

Mr. Roger L. Winblade
Manager, General Aviation Technology Office
National Aeronautics and Space Administration

Regrettably, the presentation of Mr. Winblade was not available at the time of publication. We will hope to bring it to your attention in a subsequent issue.

PERCEPTIONS ON POTENTIAL LEGISLATION

Mr. James Davidson,
Counsel, Subcommittee on Intergovernmental Relations,
Committee on Government Affairs, U.S. Senate

A word or two about the Intergovernmental Relations SubCommittee of the Committee on Government Affairs may be useful. I wish to allay any fears over what somebody from such a Subcommittee would know about the area of classification policy. Our primary jurisdiction is over the relationship between local and state governments and the federal government: grant-in-aid programs, the so-called countercyclical aid to cities program, and oversight jurisdiction over revenue sharing. But what, you might ask, are we doing in the area of classification policy?

Well, several years ago, Senator Muskie took a very strong interest in this subject and since nobody else in the Senate was doing anything about it, he just reported out a bill, and that got things started and settled our jurisdiction over that particular subject. That's the way jurisdiction is often changed in the Senate – not by any formal reorganization.

On the House side, at least the names of the Committees reflect to some extent what they're responsible for. In the Senate, our Subcommittee on Intergovernmental Relations spends about 40 to 50% of its time on intergovernmental relations problems, and about 40-50% of its time on questions related to classification policy, freedom of information, privacy, executive privilege, and any number of other subjects, including Federal Sunset legislation on which we're now working and which would require reauthorization of federal programs periodically.

Our Subcommittee, in its jurisdictional responsibility over security classification, very much parallels the House Subcommittee on Government Information and Individual Rights, excepting freedom of information. The legislative jurisdiction over that Act is in the Judiciary Committee in the Senate. But we do deal with executive privilege legislation – the question of the right of Congress to information held by the Executive Branch. We also have responsibility for federal privacy legistation.

Our Committee and the House Committee in 1974 separately held a series of hearings on classification and to my knowledge, it's the last major series of hearings dealing with classification policy that have been held in the Congress. They were a rather extensive set of hearings in the Senate – six days – they included testimony from former Executive Branch officials; present officials; scholars who have examined the area of the need for the government to protect its secrets; and scientists in the field, including Dr. Edward Teller, who came to give us his views on the need for, and time for protecting basic research efforts that are going on in the scientific community.

Since that time, there's been a diminution of activity. Not in small part because of what one might term a period of reconstruction after the Watergate era. But also in part because we have not had very much presidential leadership during that period of time. It has not been a negative attitude, but only the lack of any party focus on the issue of legislation dealing with classification policy.

We also had had a major change in the area of information policy – the amendment to Section (b)(1) of the Freedom of Information Act, which was a product, in part, of Senate hearings, that our Subcommittee had held with the Judiciary Committee in 1973. You will remember that late in 1974 the amendments to the Freedom of Information Act were passed by the Congress over President Ford's veto. These established an entirely new standard for withholding and judicial review of withholdings of classified material by the Executive Branch. As you may know, the Freedom of Information Act is not considered by the courts, nor by the Justice Department as a specific legislative basis for the executive order on classification. Rather, the Freedom of Information Act refers to withholdings pursuant to *an* executive order. And it's that concept that was strengthened in the amendments to Section (b)(1) by saying that information withheld under an executive order must be properly withheld under such order. All that (b)(1) is saying is that if there is an executive branch standard for withholding information, the Executive Branch must follow its own rules, so to speak, when it withholds material.

The difficulty we've had in the past, however, is with the courts' interpretations of (b)(1) withholdings. The most noted case – one with which you probably are very familiar – is *EPA v. Mink*. It was handed down by the Supreme Court in 1973. In that case, the Court refused to examine the memoranda relating to the Amchitka nuclear test, which several members of Congress had asked for. They discussed the environmental impact of a planned atomic test in Alaska. The Supreme Court refused to order the release of the memos saying that the Congress had not given the courts the authority to examine withheld materials to determine what material was properly being withheld pursuant to an executive order and what material was not. The Congress believed that it had given the courts that authority, even though Justice Stewart, in a concurring opinion in that case, specifically laid out why the Court believed it had not. He said, if you give us that authority, we'll use it. We took them up on it. We gave them the authority in the 1974 Freedom of Information Act Amendments and the courts still don't want to use it. They keep backing away from the concept of placing the Courts in a position of questioning the executive branch's justification for the classification of certain kinds of information.

A very famous case which touched on this point was, as you know, *United States v. President of the United States, Richard M. Nixon.* That was the Watergate tapes case in which the Chief Justice, in an aside in the opinion, expressed some reluctance on the part of the Court to look at material that had been withheld by the President, if it dealt with his foreign affairs or military affairs responsibilities. The Court said that this might even be a preserve into which the courts would never intrude, even for the purpose of *in camera* inspection. I guess what the Court meant was, it didn't trust a judge to look at this material. You in this Society deal with classified material all the time. You

know that it's not some supersecret mythology. You know that classifications are simply a management tool – a means of controlling and guiding access to information for specific purposes. In some cases, it may be very sensitive information, but you apply more sensitive controls to it. The Judiciary just doesn't want to get in the process of second-guessing executive decisions. On the other hand, the courts are not reluctant to review a complex antitrust suit, which may involve reading hundreds of thousands of pages of records to determine whether a particular company was in league with another company to fix prices. Yet this area is perhaps many times more complex than many of the decisions they've been asked to review in the area of classified materials. Nevertheless, they have expressed reluctance to get into such an area.

We have attempted to encourage court review yet another time, in a recent case before the United States Court of Appeals for the District of Columbia. It's one that I would commend you to look at, because it's going to affect, I think, the judgment of anyone who is handling classified materials. Finally, we have gotten a court with jurisdiction in this area, to acknowledge that the Freedom of Information Act of 1974 changed the standards. The case is entitled *Weissman v. The Central Intelligence Agency;* this is a case before the U.S. Court of Appeals for the District of Columbia Circuit. Gary A. Weissman sought to get some information that was collected about him by the Central Intelligence Agency. In the late '50s and early '60s, he was a student involved in international student organizations and the agency felt that he might be a very good person to provide them information because of the number of times that he traveled abroad. So they conducted a background check, and for one reason or another, decided not to offer him employment. Mr. Weissman, several years later, decided he wanted to see what the Central Intelligence Agency had on him. And so he sought to get that from the agency and the agency gave him part of it, but withheld a significant portion. That was the issue that went to the U.S. District Court for the District of Columbia and the District Court said, I'm sorry, we can't go behind the classification stamp and look at that information; we trust the judgment of the agency and that's it. They didn't conduct an inspection to see whether or not the parts withheld were properly withheld under an executive order.

The initial Court of Appeals decision ratified the District Court's decision. They declined to look at the material *in camera*, and indicated that they only were in a position to review the agency decision to see that it was not unreasonable. Well, that's not what the Act says. The Act says that you are to give substantial weight to the agency's decision, but you also must be assured that the information was properly classified according to the executive order. The court did not do that. The courts were told by the 1974 amendments to review the classification decision *de novo*. That's simply saying that they have to look at it anew. They're not looking at it from an appellate standpoint. They're not saying, agency, were you arbitrary and capricious in making your judgment? That's not the standard they were to use. They were to take the information, the agency's statements, and the plaintiff's statements and then determine if the agency followed the executive order.

The court refused to do that the first time around. Senator Muskie, in an *amicus curiae* brief, urged the Court of Appeals to rehear the case. The court did not order a rehearing, but amended its original order and acknowledged that the Freedom of Information Act Amendments of 1974 did change the standard to review and did require the courts to look at the issue anew. While the outcome of the case did not change, at least, for the first time, we have a court saying affirmatively that the Freedom of Information Act Amendments do require the courts to look at the issue *de novo*. The courts had put a lot of weight on the language in the legislative history which said that they were to give substantial weight to the agency's decision. That is fine. The agencies are the ones with the technical expertise in the area. Our concern was that the courts were simply abandoning their responsibility, and I think this opinion reverses that trend.

Why is all of this important to you? Well, it's important because the Congress and the Executive Branch must have a clear understanding of what the role of the Judicial Branch is going to be with respect to information that is protected by the Executive Branch. The way our system works, the Congress gives authority to the Executive Branch to carry out a policy – such policy is always subject to judicial review.

With respect to future classification policy, I want to highlight four areas of concern – areas of concern that I think will dominate the congressional debate over legislation in this area.

First, the limitation that classification places on any kind of informed debate or discussion – discussion not only between the public and the government over what ought to be classified, but debates within the executive branch. Ray Kline, who is a former director of the Intelligence Division of the State Department, commented that during the Kissinger era, that it was very, very difficult to – for sublevel state department officials – get access to anything, because compartmentalization kept it only at the highest levels. Someone sitting on a particular desk in the State Department might not even know what major policy agreements the Secretary of State had made affecting his area of jurisdiction because that information was held up at

the NSC level.

Such also results in a limitation on public discussion, as well. We can argue until doomsday whether the information in the so-called Pentagon Papers should have been classified. Nevertheless their release certainly contributed substantially to a more informed public debate about the nature of U.S. involvement in the Viet Nam War.

Second, I think we need – and I think we're moving in this direction – to assure that the classification process is never used as the basis for criminal prosecution. A person should know with a degree of certainty when he or she releases information whether that information is to be accorded proper protection. And if you have an administrative standard where various people's judgments determine whether a document gets a classification stamp or doesn't get a classification stamp, and you use that as the basis for criminal prosecution for the release of that document, then we have removed due process from the criminal process. Due process would require that the individual who is subject to the prosecution know with some degree of certainty what kind of material can be released and what is to be protected. That's why I think that the present espionage laws, albeit not perfect, have worked relatively well in that they have been interpreted to require a level of intent with respect to the unlawful disclosure of certain kinds of information. These laws have existed apart from the classification system in setting the standards for criminal prosecution.

Third, I think we will have to begin to explore the extent to which classification may deter certain developing technologies. Several witnesses in Senate hearings have expressed concern that technological information withheld over a period of time, can retard this country's very competitive private industry. A frequent example is in the computer field. There was a big debate after World War II as to whether we would allow computer technology to become public knowledge or keep it within the government and keep a highly classified stamp on it. Well, we released it and it turned out that our expertise in the computer field transcends any other country in the world, because our private sector developed it at a far greater rate than anyone else.

Finally, I think we need to look at the cost involved in classification. The direct cost – in terms of administering the classification system, and the indirect costs that are involved in contracting out for products and projects. We must try to assess what that means in dollars and cents to the federal government, and whether we are getting our money's worth. We can argue that it's very difficult to know with any kind of precision what kind of information is going to be in need of the highest level of protection, and therefore, a large amount of cost assigned to it. Well, I think we need to start thinking in those terms, start making judgments, informed judgments about whether we are spending too much or too little for the protection of certain kinds of information.

Those are the major points I think that we'll be debating. I anticipate that our Committee will be holding hearings sometime before the end of this Congress to renew the debate on classification policy, and it's very possible that the 95th Congress will see some form of classification legislation.

Questions and Discussion

The Chairman: We have been listening for two days of the relative advances between the United States *vis-a-vis* the USSR, in areas of technology. It appears that in many instances they're ahead and in some instances, we're ahead, and I will not make a judgment as to which is on first. However, the last definitive study that I'm aware of, as to whether classifications deter scientific progress was that made by the Association for the Advancement of Science and reported in one of our seminars in 1969. It seemed then that a closed society does in fact produce things of quality. Could you comment on whether there is a real question as to whether classification does or does not deter progress?

Answer: I must preface my answer by saying that I'm not a technological expert as you may realize. The only judgments that I can make are based upon witnesses that we've had before our subcommittee who have discussed the issue of classification as it applies to technical information. One witness who holds some very strong views in the area, is Dr. Teller. Teller is one of the real geniuses of our generation, perhaps of this century. He told us that it was his best judgment that any piece of basic research in any major field of advanced technology that may have or may not have military implication was not going to remain secret for more than about one to two years; and, if it were kept secret for more than one year, it was going to retard everybody's effort to move ahead in the field, including our own. He made a very strong distinction between basic research and the application of that research. For example, basic research in the area of laser development and the application of that research for any form of weaponry -- he believed the latter category was properly protectable and for whatever period of time that was determined to be necessary. Now, to go from basic research to technological development, one of the increasing difficulties in this country has been our inability to hold on to our computer technology. It is one of our key chips, if you will, in any negotiations with the Soviet Union and other countries. But to the extent that our infor-

mation is leaking out through other sources, that impairs our ability to use it in negotiations. We have not received any testimony on this issue, but other Committees in the Congress have begun to look at the amount of computer technology being funneled through contracts to independent or neutral countries, who, in turn, sell or deliver that same information to our adversaries.

Question: Pursuing, what you started to get into on the foreign release of technology, and your statement about administrative processes for criminal sanction, are you familiar with the International Traffic in Arms Regulations? In them, there is a definition of technical data and the most ill-defined and poorly used definition of how to control technology that I have ever seen. People who are involved in international operations run the risk of violating this and being subject to criminal sanctions, and administrative sanctions under the new procedure which was proposed by the Office of Admissions Control. Has your Committee looked into this, to see if this is stifling U.S. industry in their attempts to operate overseas?

Answer: Our Committee has not. The jurisdiction for that legislation is the Foreign Relations Committee, and it's also shared, in part, with the Armed Services Committee. Our Committee has not looked at that legislation. We have no jurisdiction whatsoever.

Question: For many years, there's been a pull in opposite directions on the subject of rights of individuals versus rights of society. In the case of ordinary crime, for example, we see or find many cases where criminals are out on the street because their rights have been protected as individuals, but society is suffering as a result. The same situation applies in the classification area, and there are many who are pushing hard for the protection of individuals' rights, such as in the area of "freedom of information." And in the case of the rights of the people as a whole to protect necessary information, there are sometimes serious problems.

For example, the government has repeatedly let people go, not prosecuted, people who have released classified information, because the very course of trying them on the charge would release more information. Has your Committee thought about this problem? Has, it, for example, considered the value of a United States Official Secrets Act, or some other method to protect the rights of people, as a whole?

Answer: We have thought very extensively about the adoption of an Official Secrets Act, and quite frankly, have fought it at every single stage that it's been proposed. And we will continue to fight it at every single stage that it is being proposed. The criminal system in our country is subject to criticism – and it's very difficult to justify in many people's minds why someone goes loose on a "technicality" in this country when they appear to have committed a crime. However, a fundamental element of the system is that we've got a very unique set of amendments to the Constitution; the first ten I think are probably more important than the criminal laws of this country. They secure rights to you and to me and also to those individuals who may or may not have committed a crime, but are not prosecuted by the system. They secure for all of us a measure of protection that is not enjoyed by anybody else in the world. And that's what makes this country great. One of our concerns was over S.1, the proposed reform of Federal Criminal Code; the current draft of which, I might note – that's been worked out by Congress and the Justice Department – no longer contains amendments to the existing Espionage Laws.

Under one of the proposals that was made earlier, an individual could have been prosecuted for the negligent release of information that had a classified stamp on it. Just think for a second about the most unjustifiable confidential stamp you've ever seen on a document, something that you knew did not merit classification. As you go home at night you take some papers with you and on the bottom of that stack of papers was that document that had the confidential stamp on it; you put it in your car and then you get out of your car, go home, and the paper falls on the ground, and somebody else picks it up.

At that point under S.1 as drafted last year, you would be subject to criminal prosecution. That's insane! There was no intent by you to harm anyone at all.

It is equally difficult to base a criminal prosecution on the intentional *release* of a document that bears a classification stamp – even though the document has gone through all the proper classification channels. Because the standard which you apply for the administrative control of a document should not be equated with the judgment a jury must make as to whether the release of the document could reasonably harm the United States.

Now we're talking about the intentional release of that information – to someone who doesn't hold a classification rating commensurate with the document. Would you want that person subject to criminal penalties of between three and ten years? S.1 would have provided that; whether or not the document should have been protected at the level that it was marked, whether or not it would ever have caused any harm to the United States, or given any advantage to any foreign country; the fact that it bore the stamp would have been the basis for the prosecution. The point that I'm trying to make is, that the criminal statute itself

should set the standard for the release and protection of the document – not a statute or executive order that in turn tells somebody else to make a judgment about how the materials are to be protected. Anything else is antithetical to the way our criminal system operates. We have been told by Justice Department prosecutors, there have been lost prosecutions, because of the government's judgment in a case not to go forward, because it would require the release of more information than they were willing to release in order to get a prosecution. That's an inherent difficulty that will always be with us as long as we assure that an individual has a right to a public trial, as guaranteed by the Sixth Amendment, and as long as we are going to maintain our concepts of basic due process in terms of the standard by which we hold a person accountable for criminal conduct.

Administrative sanctions should be sufficient to enforce the classification system. When you're talking about putting somebody in jail for one, three, ten years, or holding them to the possibility of life imprisonment or a death sentence, then I think you have got to be very, very careful about our constitutional guarantees of due process.

Question: How then do you protect the true secrets from the true culprits?

Answer: The true secrets and the true culprits are something for a court of law to determine in this country. Not for you to determine, not for me to determine, not for anybody else to determine, but for a jury of twelve peers of that defendant, according to a legislative standard for criminal prosecution. It's worked, not perfectly, but better than any other system that I know of, for many years.

Let me just offer you an example of how important this is to the Congress' and the public's concept of due process in this country. You probably know very well that our first major set of espionage laws was passed in 1917 – that's a very familiar year, I think, to most people in terms of U.S. conduct in foreign affairs. The second set was passed in the late '30s and early 1940s, also another fairly tense period with respect to our relations with other countries. You would expect the toughest set of laws imaginable would be passed at that time. Yet with all of them, except certain classes of cryptographic information and other information that is *specifically set out in the statute*, with respect to all the others, a high level of intent to harm is required of the defendant. The Congress, at the height of some of our worst conflicts with other nations, at the height of concern for the protection of military information, was not willing to give up a basic fundamental standard of due process in the area of prosecutions for the release of that information.

Question: I'd like to make a comment and then ask a question, if I could. The comment involves the earlier observation about Restricted Data and Dr. Teller's views. I don't want to get into a dispute with Dr. Teller, but over the years there has been tremendous volume of Restricted Data declassified by the former Atomic Energy Commission – now ERDA – and you can get into an argument about what's basic research and what's applied research. But from my standpoint, we really don't classify basic research; so I would like to clarify that point.

The question is – and I'd like to ask for your personal opinion – that there's a great volume of technical information that is generated by government support. It's high quality technology. In our area, and I'll speak from our area, much of this information is not classified. It doesn't have a national security aspect to it. Therefore, we're obliged by the Atomic Energy Act to publish it, disseminate it widely, and that means both in this country and abroad. Would you support a statute that would recognize, say, something like government proprietary? That is, information of high technical quality that was generated by government dollars to allow some sort of control over it so that it wouldn't flow freely to other countries? The situation that we have today is that we have that information, it's generated and we publish it. This puts us at a disadvantage, because when we get into negotiating bilateral agreements where we exchange technical information, it's difficult for us, because some of the countries can just sit and wait and they'll get our information without any sort of a *quid pro quo*. And so, back to the question, would you support some sort of statute which would admittedly give safeguards and precautions so as to assist in retaining some technological advantage?

Answer: Fortunately for me, and probably for you, it doesn't matter whether I support it or not. It's whether or not the Committee and the Congress support it. But the point I was making earlier with respect to the export of highly technical information to other countries, was directed at this issue. I think the Congress needs to start examining this whole area of the export of highly sensitive technology, whether or not it does "damage" to the United States. If we are going to use this information as a technological bargaining chip, it does not make much sense to permit the free dissemination of that information.

That's the point I was trying to make. I don't know enough about the area yet to make an informed comment as to whether we need such a statute or don't.

Question: I find it extremely difficult to appreciate the reluctance of the U.S. Congress to draft legislation for an Official Secrets Act, when our British Allies have had such an Act on the books for almost 50

years or more. The United Kingdom is certainly not a dictatorship – they are the cradle of western democracy and their legislation has been very effective in protecting the rights of society, their society. Furthermore, their act also covers the loss of classified documents, and to the best of my knowledge, no Briton has ever been sent to jail for – as a criminal sanction – for something that was beyond his control. Would you care to comment on this?

Answer: I would because I feel very strongly about it – if you didn't gather that from my earlier comments.

We have spent considerable amount of time – in the neighborhood of 75 to 100 hours – in discussions with officials of the British government with respect to the Official Secrets Act, and examining their experience under their legislation. They were interested in the way our system operates and they established a Commission which examined our system as part of its charter. *But* let me just point out one small distinction between their system and ours. They don't have a constitution and we've got one with ten very important amendments to it. Their concept of an Official Secrets Act is very difficult to square with our Constitution. Our concept of a free press doesn't comprehend an Official Secrets Act at all. Witness the *New York Times* case. The Supreme Court in that case upheld the First Amendment as an absolute bar against issuing an injunction against the publication of any information. The First Amendment says Congress shall make *no law* abridging the freedom of the press. There is no other country in the world that has that and implements it the way we do. And also, there is no other country in the world that enjoys the freedom of individual thought this country has.

PERCEPTIONS ON POTENTIAL LEGISLATION

Mr. Timothy Ingram
Staff Director, Subcommittee on Government Information and Individual Rights,
U.S. House of Representatives

Following Jim's approach, I thought I might share with you today a little background relating to the Subcommittee, what its responsibilities are, a few comments on what it is doing now, and then touch on what may be our activities in the near term.

We have an interesting Subcommittee with quite a history – about 20 years with John Moss, who was a very active Chairman of the Subcommittee and was responsible for the Freedom of Information Act, among other laws. The FOIA still gives agencies problems and we still hear about them. We have the Privacy Act within our legislative jurisdiction and it's creating problems of its own since it doesn't quite mesh with the Freedom of Information Act in places; as some of you may have noticed. Then, there's the Federal Advisory Committee Act and the Government in Sunshine Act, which we managed to get through last year. The latter particularly is causing a few problems as well. It has been in effect only a few months and we probably will be asking why some of the meetings are closed in some of the regulatory agencies. Probably also, we'll invite the President to do the same – on one or two occasions – just to learn the reasons why particular meetings are being closed and whether appropriate transcripts are being kept, and so on. So, we have responsibility for those four Acts and we have oversight over about seven agencies as well – to look at their economy and efficiency of operations. The agencies are the Justice Department, the U.S. Information Agency, the Government Printing Office, the Postal Service, National Archives, Federal Communications Commission, and the Veterans Administration; there may be others less well known that I haven't covered.

To accomplish our tasks we have only five staff people including me – we're spread a little thin. Because of the scope of activities, the staff tends to the generalist approach. I personally have no pretensions to detailed knowledge in any specific field. For that reason it's always a pleasure to be with a group who have some particular expertise, and have an ability to focus on some particular tasks.

The committee has several planned activities that I believe may interest the Society. For example, there has never been a really workable *regional* implementation of the Freedom of Information Act. During the ten years that it has been in effect we have inquired of the agencies in *Washington* asking about their implementation of the program. We have a great deal of information reflecting on that activity. But, we have never gone to *Cincinnati*, say, to see whether anyone out there has ever heard of the Freedom of Information Act and what a citizen request for information really means. So, we've asked the General Accounting Office to look at the operation in about ten different cities. Depending on the results, we may need to visit a few cities to learn whether the regional offices of the various Federal agencies are implementing the Act and how they are doing it.

Another aspect that has long concerned us, and we are now finally getting around to taking a hard look at it, is business and corporate use of the Freedom of Information Act. This may get a little closer to home. Reverse FOIA cases have grown up over the years. For example, consider a potential type of case: *Alka Seltzer* will go into court to try and get an injunction against the Food and Drug Administration to prevent the release of information that *Alka Seltzer* has provided them. Frequently such an action will be before a

Federal Judge who may have a background in corporate law. The corporation will attest that release of certain information will damage their competitive position as well as cause financial losses. An injunction may then issue against the FDA to prevent release of specified information. In many cases such injunctions are quite legitimate. Trade information is proprietary and could have monetary value to *Alka Seltzer's* competitors. The Freedom of Information Act may provide an easy way to get competitor data by making an FOIA request for certain information that the various agencies may, because of law or regulation, have on file. So, we need to examine how that process has worked out. Of course, the reverse FOIA case situation was not contemplated when the Act was passed. It was thought that there would be an outflow rather than a restriction on the release of information. As a policy matter we want to see whether the Act serves the purposes planned, or whether it works at all in such cases. If not perhaps we consider what limitations should be placed in the Act. Consider a different situation. Government procurement lawyers, as a whole, perhaps are not that familiar with the Freedom of Information Act. Consequently, when drawing up a government contract they may not be thinking about the nuances of having across from then a corporation attorney who may be thinking "What if my competitors make an FOI request for this contract. What's going to happen to me?" Usually the contracting attorney drawing the contract will want to be as specific as possible about a particular method of construction, say, that the given contractor is to use – a method that may have been the basis for the award of the contract in the first place. Allowing a competitor then to gain access to such information would not be appropriate. Perhaps we need to put together some suggestions for government procurement lawyers to cover such situations. We have concluded that there probably is a need to examine the effect of the Act on the industrial community, particularly as it relates to trade secrets and proprietary information.

In another area, we recently sent a questionnaire to the executive agencies relating to administrative markings and the use of such markings by some agencies in place of, or in addition to, Executive Order markings. Over the years some agencies have developed their own security system, in effect, for handling sensitive information. We would like to learn how many different types of markings are being used and the effect they may have on a Freedom of Information Act request; for example, suppose a citizen makes a request for information that is marked "Eyes Only." Is there an internal regulation that requires the FOIA Officer to go back and check with the originator of the stamp before a determination on release? How much time does that add to the whole process? We need to consider that kind of question. The questionnaire is similar to one we sent out some 5 or 6 years ago. It is probably time to see whether there should be some across the board relief from some of the administrative markings that the agencies are using.

Then moving to future plans, our thought now is to start holding some hearings later on in the summer or fall in oversight of the (b) (1) exemption to the Freedom of Information Act to see how the Courts have been interpreting the amended section; to see how the agencies are handling their FOIA requests; and, then to go on from there to a more general oversight of the classification system. We plan, of course, to keep abreast of developments in the executive branch in revising EO 11652. Related to the classification system, Senator Biden's subcommittee of the Senate Intelligence Committee, is taking a look at certain aspects – particularly the quality of damage assessment reports put out by the agencies; questions of leaks, and probably some questions relating to compartmentalization. That committee probably is in a better position than ours to raise some questions because of access – at this time it's better than ours.

A problem that we have always faced on the Hill is that we really have no Security Officer. If I want to find out how sensitive information is handled and safeguarded, I either have to go to one of the executive agencies and ask for their advice or use my own best judgement. So I think another thing that we'll be considering is where are we respecting the responsibility of the Congress to establish procedures for the receipt of sensitive information. A related topic that we're working on now is the Justice Department's policies for providing information to the Congress. One finds that with a new administration there is an interesting kind of education process. Reinventing the wheel suddenly becomes a part of it. We are trying to work out now with the Justice Department what their policy should be about when they can give us information and when they can't and under what circumstances. The arguments are the same as we've heard over some number of years, but the people are new. It's likely that some of you are faced with a similar situation regarding new people and security classification. They have to be educated from the start. This is an under-standable part of the process in this government because there is, essentially, a limited contract for a few years of service and one must re-establish the ground rules from time to time.

This, then, is an overview of our Subcommittee's activities and what kinds of things we may be doing in the relatively near-term.

Questions and Discussion

Question: Is the committee viewing some hearings concerning the different legislative proposals previously submitted either as a legislative base for security classification or for further restrictions?

Answer: No. At this time only one or two members of the Subcommittee have been with it very long, so even in it there is need for the education process, starting with such basics as the committee's jurisdiction. As a practical matter, we will proceed very slowly in terms of what is a congressional oversight job; starting with the Freedom of Information Act – particularly the (b) (1) exemption. Any other course would not be realistic at this time. We do have some new members who bring to the committee a substantial background and knowledge. However, we will probably start slowly with some educational hearings that will be useful for the members and leave our options open. Our new Chairman has a broad judicial temperament and background and has created a fine atmosphere within the staff and the committee.

Question: Is there a secrecy code or is there a procedure by which information furnished to the Congress is protected?

Answer: There is a procedure known as receiving testimony in Executive Session. It requires a formal vote by the committee to receive oral testimony in Executive Session. As a practical matter, most committees will abide by the recommendations of the executive branch agency furnishing information about its sensitivity.

Question: Are you saying then that the rules of the committee provide for handling classified information?

Answer: Privileged information. The view has always been, in practice at least, that the committee or member who receives information will respect or take into consideration the recommendation of the executive branch agency which submitted the information about the level of its sensitivity. Again, and on the other hand, there would be no penalty to a Member of Congress, nor as a practical matter, to his staff for the inappropriate release of information. As I said, unless there has been a violation of the Espionage Act there is very little sanction that can be imposed. I think that one of the things of legitimate concern to the executive agencies is that there be a uniform procedure by the Congress for the receipt and handling of sensitive information. The rules vary from committee to committee. Whether there should be differences, I'm not sure. On the whole however, and with few exceptions, the material has been handled properly. As I commented, there is no Security Officer in either the House or the Senate a staff person can go to for advice on the physical handling of information received from executive agencies. The difficulty on potential releases is the exercise of judgement by the individual members and the amount of their sophistication in terms of understanding the legal implications of what classification markings are. On the opposite side of the release coin, I have had calls from members – newly elected and not – wanting to know whether they could read classified information that was put in front of them. I'm not saying that this is the way things should be, but a Congressman should have access to any piece of paper he wants, as a matter of constitutional right. As an aside, there is a constitutional question of whether an individual representative or senator cloaks himself with the power of the House or Senate when requesting information, or whether there is a higher status accorded a committee's request. Similarly, does the request of a committee chairman have more weight than that of a committee member? And, does classification play a part?

Question: No one questions the right of a congressman to ask for an receive information. But, a related question and concern is what sort of protection is given to the information? What sort of facilities does he have to secure it? How are these things handled?

Answer: For example, I have in my office two safes approved by GSA for the storage of information up to the level of Top Secret. The safes are used to store classified information requested by the Committee.

Question: Do you think that in some measure inappropriate releases by relatively new members of Congress could be characterized, on balance, as a lack of education; a lack of understanding; or a lack of a place to go to inquire? For example, an individual member takes it upon himself to determine that the 9 kilohertz frequency of a particular missile seeker is not really important because he really doesn't understand its purpose. Is there any merit, or could there be, in some kind of an education program for the Congress; or is there any desire for such?

Answer: I think that what you suggest is something that in addition to the other nine points that are given to a member when he takes office there be some suggestions and guidance regarding classified information. It is a matter that we'd like to examine in our hearings. Learn in greater detail what current procedures are in use, and possibly make some suggestions for the handling and the receipt of privileged information. As I mentioned, the practices vary now from committee to committee depending on committee assignments of the particular member. Consider for instance, whether the Agriculture Committee ever would receive classified information and whether they would know what to do with it if they did.

Question: You commented about what might be termed Freedom of Information Act requests affecting the industrial community. Would your committee be concerned or are you concerned about the fact that there is a sort of gap in security policy or regulation in the executive branch. We do not really protect proprietary information in the executive branch. Some other examples of information on which there are similar difficulties include criminal investigative infor-

mation, foreman information, grand jury information, witness information – all of which generally is exempt, it's true, from the Freedom of Information Act. What do you think would be the reaction of your committee if the executive branch tried to put out some sort of general policy to identify and protect that kind of information? Have you thought about this? We in the executive branch have sort of been burned by the newspapers for trying to withhold such information.

Answer: Let me sort out what I think you are saying. Part of the rationale for sending out the questionnaire on administrative markings that I described, is to see how agencies are now attempting to cope with the handling of sensitive information which would not meet the requirements of the executive order for security classification. In that connection, it will be interesting to see how and what impact the Attorney General's recent memorandum on the FOIA appeals has. Now he is saying two things:

- Does the document fall within one of the nine exemptions of the FOIA? If not,
- Is there a very strong policy reason for non-release of the document?

Again, that's cutting across applying any kind of blanket standards, I think; but insisting that there be a case-by-case examination of particular information. There is that kind of balance there in terms of applying a very broad stamp to different types of information. I think that the Justice Department, for example, will have certain types of information – informants, and so on – where the treatment would differ, certainly, from other types of information that they receive. It is something that the committee hasn't examined; but there is disparate treatment, perhaps, of some of that kind of information. There is concern but precisely what should be done is yet to be determined.

(Ed. Note: Mr. Ingram's presentation was actually made before a meeting of the Washington Chapter of the Society on the 21st of June. Illness had prevented his presenting it at the time intended. Since it is an important part of the picture, it is included here as a part of the Seminar proceedings.)

Prize Winning Essay

CLASSIFICATION VS. CLASSI–FICTION

Arthur E. Fajans
Directorate for Freedom of Information and Security Review
Office of the Secretary of Defense

Neither secrecy nor disclosure is mentioned in the United States Constitution. The protection of records or information, principally through security classification, was established by executive order. In the past, the Congress has accepted the requirement to protect national security information and has tacitly sanctioned executive secrecy. However, secrecy is not beyond reproach for since the early 1950's, it has come under varying degrees of attack. Presidents Truman, Eisenhower, Kennedy all issued executive orders to create the machinery necessary to protect sensitive documents and all were unpopular with the press. Congress after several abortive attempts sought to limit executive control of information with the passage in 1966 of the Freedom of Information Act. Congress remains concerned about what it feels is excessive executive control of information and is perpetually considering legislation which would reform the security classification system. President Nixon's Executive Order 11652 preempted Congressional action in this area in 1972 and attempted to preserve the tradition of executive prerogatives in security of information matters.

The arguments for secrecy and the protection of information are well known. Fundamentally, it is not a question of keeping the American people from the light, it is a question of keeping our would-be enemies in the dark. Consideration must be given to safeguarding information which, if disclosed, could reasonably be expected to cause some degree of damage to the national security. Conversely though, information about our national defense posture must be given to the American people. A natural tension exists between these two principles of action and a reasonable balance must constantly be sought to maximize both objectives. When these principles collide it may leave many baffled, confused and skeptical. Justice Stewart once said that "security can be preserved only when credibility is truly maintained." Our security classification system has become to many people an "incredible" system.

> "But the military, by its constant penchant for secrecy, erodes whatever public confidence it may ever hope to have." Congressman Michael J. Harrington, Massachusettes

This does not mean that the framers and implementers of our current system are incompetent, it merely emphasizes the enormity of the complex and largely subjective issues involved. What system might you envision? What definitions would you give to "Top Secret", "Secret", "Confidential"; or for that matter, how would you differentiate between "classified" and "unclassified".

A review of the security classification system since Calvin Coolidge confirms the constant need to restructure the classification system. Each change has served well but never well enough to preclude extensive restudy with subsequent conclusions to modify existing procedures and policy. The constant failure to realize strong concepts and definitions has been regrettable. The lack of coordination, the scarcity of cooperation, and the virtual inability of the system to change its shape remains a concern. Analytical decision-makers refer to it as "sub-optimization", but there remains a tendency on the part of classifiers, both original and derivative, to become fierce defenders of the classification faith, often to the detriment of the objectives they are trying to reach. Popular feelings of alienation, indifference, and "no confidence" about much that is classified is caused by the increasing dysfunction of the security classification system. The ultimate "no confidence" results in acting in defiance of the system – also known as "leaks".

> "I personally feel our democracy is under assault . . . and unless we can turn the tide we will lose the system of government we presently enjoy. And the single item that will be responsible for this loss of government . . . will be secrecy itself and nothing more, nothing more complex than that, because secrecy is anathema to democracy. It is that fundamental." – Senator Mike Gravel, Alaska.

Some feel that there is safety in numbers and that a system of classification review by committee would provide an opportunity for every point of view to get a fair hearing. It has not proven so in the past. It is better to have fewer engaged in policy-making and policy interpretation, to have their work subjected to continual study and review, and to place them in a clear pattern of regularized reporting and responsibility. It is impossible to prevent all corruptions of a

system solely by structural design but some structures are less liable to corruption than others. These are structures that are open to public study, that are subjected to periodic review, that provide access for the public served, and that are fully responsible and accountable and accountable to legitimate pressures.

It is recognized that humanly devised structures inevitably become obsolete and survival oriented. It is further recognized that the power of implementing programs becomes dispersed and dissipated in any bureaucratic structure. But care must be taken never to lose accountability, for without accountability there will be no responsibility.

Security classification is not an exact science. Classification assigned to a particular subject or a specific element of information is a subjective determination on the part of the classifier. He may also classify information in accordance with some fixed guideline – a guideline that someone else subjectively determined. Reasonable men may reasonably differ in their perception of information which, if disclosed, "could reasonably be expected to cause damage to national security."

The Information Security Program currently embodied in DOD Regulation 5200.IR, is a theoretically sound system. To make it work, especially to the degree of refinement and speed users require, is an issue of a completely different dimension. How it appears to those outside the system is yet another question.

The Security Classificaton Guide, one of the major control instruments of classificaton management, is never current enough to reflect yesterday's, last month's or even, on occasion, last year's decisions. The guidance remains too broad. At best, classification guidance is no more than expression of intent. It cannot and should not be applied mechanically or interpreted literally. It has been suggested by some classification experts that if the guidance were more specific, they would be inundated with constant requirements to promulgate changes to the guides. The system lacks accountability. It is an artful, well-ordered structure to manage the flow of information, and in this objective, it is successful.

The Information Security Program is essentially an in-house control instrument. It sets the rules for those playing the game. These rules are not applicable, nor are they comprehensible, to the public – they were never intended that way. The objective of the Information Security program, specifically how the Military Departments view it, is security. Progress becomes movement toward attainment of that objective. If the objective is attained, security is said to be successful. The use of this measure of success is relatively empty in much the same way that one would say that the goal of life is death.

> "The record of the Department of Defense in this area is uniformly on the side of secrecy....It is my own judgment that 90 percent of what is classified should not be. Physically, there should be just as many people employed by the Pentagon declassifying material as there are classifying it." Congressman Otis Pike, New York.

In order to accomplish a balance to the protection of information, an objective review is required. This review function serves best when it is as familiar with the system as the classifier, yet is not subject to the restraints imposed by the mindset of a "protector". The act of classification is simple and rapid; declassification is involved and tedious. The motivation required for declassification is scant in a program which espouses security. There are conflicts extant in various Department of Defense policies and procedures which obfuscate and confuse. Under the Freedom of Information Act, if a request is made for any classified document, proper response must be made to the requestor explaining why he can not have the document if the decision is to deny. This response can not be made reasonably unless the document is reviewed and a determination made that the classification is in fact still valid. Yet, the Department of Defense regulations which implement Executive Order 11652 and the National Security Council Directive governing the classification of material, state that no classified document needs to be reviewed unless it is ten years old. Resolution of these baffling policies needs to be made.

There are many instruments in the arsenal of protection but there appears to be none in the arsenal of release. Unless a more reasonable balance is struck between these two principles of action then we face the assured destruction of the legitimate flow of information to the public. The "protectors" will have won. It is essential that the Department of Defense be persuaded that a freer flow of information is, in fact, beneficial to attaining the objectives of the Department of Defense – there are too many people in the Department of Defense who just don't really believe that!

> "It is generally agreed, I believe, by many of this body and the public that the classification procedures of the executive departments have been grossly abused and that they are a serious obstacle to the efficient conduct of the public's business." Senator Fulbright, Arkansas

Comments in the press and in Congressional hearings demonstrate that deficiencies exist. *It takes too much time,* is the most frequent complaint. The necessity to use appeal procedures in many cases is also described as frustrating.

There may be as many as thirty or more control caveats in use by Department of Defense components which would have difficulty in finding their official authorization. Some samples would include such labels

as sensitive, proprietary, no distribution outside the department, personal, eyes only, non public, and not public information. While there might be good and proper reason to withhold information contained in documents bearing these notations, the fact remains that these caveats are not authorized nor is there a single administrative entity in the Department of Defense to unify policy on such matters. The fragmentation of authority to exert sound management, consistent criteria, monitorship, policy development, procedures and interpretation has resulted in "CLASSI – FICTION".

There still remains a tendency within the Department of Defense to perpetuate security classification on the basis that the classification was valid when originally applied and for that reason should remain classified. Reluctance is exhibited by classifying officials in making the determination as to whether the classification remains valid in the present context. The transient nature of cognizant officials militates against an aggressive declassification and downgrading program. The assumption, all too easily made, that the original classifier must have been aware of circumstances requiring the classification decision that are unknown by the present incumbent, therefore the incumbent is reluctant to change that original decision. Even if the incumbent was adventurous enough to desire change there is no one to whom he may make appeal or seek guidance outside the security system. National Security Council Directives, Executive Orders and Department of Defense Regulations notwithstanding, the public remains faced with a security classification system which is, in practice, essentially stagnant. It can also be concluded that lack of knowledge in these matters on the part of many Department of Defense officials creates an atmosphere of procrastination, anxiety, insecurity, and just plain recalcitrance to change being careful never to let facts obscure truth.

Although the machinery that exists to process information requests (including those specifically identified as Freedom of Information requests) are adequate and responsive, the public still expresses frustration in obtaining information. Expressing the public view are the news media, special interest groups, research scholars, historians and the Congress. The most constant reference is made to time delays and the necessity of appeal when information is denied. For full perspective, it must be noted that these references to deficiencies are directed broadly government-wide and that the Department of Defense has been identified by some users as better than most agencies. The fact remains however, that the Department of Defense implementation is fragmented and that causes unevenness in just how well the job is being done. It is my belief also that time delay and denial/appeal procedures actually reveal only one deficiency, that is, some information is unnecessarily withheld from the public view.

Security classification remains an imposing obstacle to the flow of defense information to the public. Being careful not to make judgments on the efficacy of the Information Security Program, certain changes must be made in the classification review procedures outlined in Executive Orders, National Security Directives and Department of Defense regulations which are in conflict with the law as expressed in the Freedom of Information Act. Principally, the 10 year mandatory review requirement must be clarified sufficiently so that it may not be used as a shield to hide behind. It must be made clear that the intent is to ensure that information is not being withheld for improper reason or to avoid embarrassment to the administration. By placing the control of classification review actions only in the hands of the "protectors" creates a conflict of interest. Public accountability must be established as a proper and legitimate counter balance to the forces charged with the responsibility of withholding information.

An informed citizenry with faith in their institutions is essential to the maintenance of our representative form of government.One precept to be restored is that the government's case for a measure of secrecy is not frivolous or self-serving. The implementation of the Freedom of Information Act within the Department of Defense and the Information Security Program explicitly must be placed in the perspective of the availability of information and not the restraints on public access. There is need to bring unprecedented full-time attention to the Security Classification Management task in the Department of Defense and effect dramatic results in the removal of impediments to the legitimate flow of information to the public.

Security Classification has the attention of the press, public interest groups, the Congress, the courts and citizens in general. Their attention to these matters will increase. Throughout the history of the United States, the American citizen has always had a desire and, under the constitutional guarantee of free speech, a right to know about the activities of the forces raised to defend the country. Thomas Jefferson expressed the attitude in 1799 when he said:

> "Your fellow citizens think they have a right to full information, in a cause of great concernment to them. It is their sweat which is to earn all the expenses of the war, and their blood which is to flow in expiation of the causes of it."

The programs, procedures, and administration are all there. No vast changes to the varying programs is required. No new reorganization is envisioned. Only increased individual energy and expertise is needed to identify and remove obstacles, confusion, duplication, redundance in policy and procedure in order to improve compliance with existing law, directive and

regulation. Buried deep within those existing laws, directives and regulations is a directive that you challenge security classification determinations – challenge them again and again. Don't accept the Classifier's Soliloquy:

To classify or not to classify: that is the question.
Whether 'tis nobler in the mind to suffer
The slings and arrows of outraged news reporters
And to invoke Executive Order 11652
And so by exemption protect information. To declassify, To disclose
No more; and by a thirty year exemption we end
The heartache and the thousand natural shocks
The classifiers are heir to. 'Tis a consummation devoutly to be wished . . . .

'Tis a consummation devoutly to be avoided. Put the "a" legitimately back in Classific_tion.

PATIENCE AND THE IMPORTANCE OF BEING REDUNDANT

Mr. Donald Woodbridge
KMS Fusion
Counselor of the Society

Back in April I made a pilgrimage to Germantown to attend a meeting and commune with colleagues in the ERDA empire – the Energy Research and Development Administration, that is. I liked to think of them as colleagues for old time's sake, and I persisted happily in that view until on this latest occasion, I was humiliated by having to wear a badge that said ESCORT REQUIRED. The reception-person at the desk couldn't care less that when Q-Clearances were first handed out many years ago Woodbridge was among the first to get one and that Woodbridge had been trusted with a Q since before she was born. (Actually that is a bit of flattery.) The humiliation was mitigated somewhat by the charm and good nature of the escort-person assigned to share the elevator with me and take me down to the cafeteria at lunch time. The escort-person did not join me for lunch, however, and for company I had to make do with Bram Feldman and Ignazio Cucchiara (better known as Cooch) of the DOC whom I spotted lingering over the remains of their epicurean repast. For a brief spell I felt once more that I was among friends and colleagues; and then I had to ask a guard to request my escort-person to take me back to the fourth floor. *Sic transit gloria mundi.* (No, her name was not Gloria.) Why after these many years was Woodbridge suddenly *persona non fidetur,* if not *non grata?* I felt a kindship with J. Robert Oppenheimer and a special spympathy for Hawthorne's heroine Hester Prynne of *Scarlet Letter* fame. Shakespeare's sonnet No. 29 kept running through my mind.

When in disgrace with fortune and men's eyes
I all alone beweep my outcast state,
And trouble deaf heaven with my bootless cries...

Since we arrived in Alexandria, I have been haunted by another Shakespeare sonnet:

Shall I compare thee to a summer's day?
Thou art more lovely and more temperate
Rough winds do shake the darling buds of May
And Summer's lease hath all too short a date.

If you have a penchant for conspiracy theories, your imagination can have a field day. After the meeting I said good-bye to the convoluted corridors of ERDA, muttering to myself a paraphrase of an advertising slogan sponsored once upon a time by my erstwhile employer, Union Carbide, "If you can't trust Woodbridge, who can you trust?" I always thought Carbide was badly advised by the advertising agency in letting loose on the television screen that crew of fur-clad north-country skeptics obviously already inoculated with distrust of Prestone, albeit hopeless of finding anything more trustworthy in the arctic air. If you can't trust Woodbridge, who can you trust? It's a good question and I don't know the answer. After yesterday, you know how far we can trust Robinson & Bagley.

Those of you who failed to make good your escape on past occasions when you saw me on the speaker's platform will have noted that trust is a recurrent theme in my discourse. There are the congressmen to whom honor means nothing; the workers in think tanks who say they answer a higher call when they purvey to the media information they have sworn to protect; the statesmen who use the leak as a tool of power. The ravelled thread goes on ravelling. And now we can rejoice in a president who has promised never to lie to us. It makes one marvel. And we know he will not give away our secrets, since he is the final arbiter of what is secret.

Μὴ θευμάσῃς ὅτι εἶπόν σοι, Δεῖ ὑμᾶς γεννηθῆγαι ἄνωθεν

Which, translated from the Greek, means "Marvel not that I said unto thee, ye must be born again".

By the way, did you see the cartoon in the Wall Street Journal showing Diogenes, lantern in hand in his hunt for an honest man, face to face with a chap who says, "I am the guy who tells the truth that lies somewhere in between"?

In this 13th Seminar we have confronted a different sort of trust. It is more like trusting Prestone than trusting Woodbridge. Can Classification be trusted to do the job? We have to be sure, in reviewing legal and legislative proglems, given thought to how to re-

compense the untrustworthy, but our main concern has been to examine the practice of classification, what the AEC called the mobile and dynamic art, to learn whether classification provides a framework we can trust, quite apart from the morality and integrity of those who are entrusted with classified information. Is classification indeed the cornerstone of security – or is it the millstone? With this theme we have harked back to the seventh seminar and your patience has been rewarded by a spendid exhibition of redundance or, if you prefer, by an exhibition of splendid redundance.

Jack Robinson has given me a dandy title – much better than my overworked view from the sidelines. Patience, and the importance of being redundant. He gives me license to repeat myself, and enjoins you to be patient while I play with words.

He that hath patience may compass anything, according to Rabelais. And Buffon tells us that genius is nothing else than a great aptitude for patience. So be patient while I take you back to the Statler Hilton in July of 1971: 1971 was the year of Daniel Ellsberg; the year of the self-employed classification consultant; it was the year NCMS almost made it to national television; it was the year that George MacClain said the motto is no longer when in doubt classify, the motto is when in doubt find out; it was the year that Jim Bagley said that NCMS came of age. And let me quote from the NCMS *Bulletin* of that time:

> "Most of us will agree. We no longer talk just to ourselves. Out in the world, people are beginning to listen, to look, to wonder hopefully, I think, whether this Society can and will contribute new and creative insights, exercise unfettered skills, bring plain and simple common sense to bear in working to extricate the security/classification service from the legacy of past mistakes. Signs of our progress toward maturity are the character of this past seminar, the strength of our cooperation with colleagues in government and recognition in Congress of the potential of NCMS."

In the 7th seminar, as in the 13th, a distinguished group of scientists and policymakers considered what kinds of information ought to be classified, and the conclusions of the two groups are very similar. Protection of lead time, the futility of trying to protect information after deployment, the need for developing rationale – specify why something is classified – the importance of separating military and technical areas from political matters in imposing classification. The needs and criteria have not changed essentially, though I thought I detected a new emphasis or, perhaps I should say, a more increased emphasis in today's criteria on the usefulness of declassifying information to enhance credibility. It gives one pause to realize that we are at a point today where we must play that game.

Redundance – but highly important redundance. In the midst of the routine, the stamping and marking, the 254's, the counting and costing, we need to be reminded of the basics, to take another look at the fundamentals, to see classification as a highly intellectual activity. (I am sure you applauded, as I did, when Don Loofts pointed out that it takes more than clerical personnel to handle the tasks we face.) Such a look and such a reminder are what the Thirteenth Seminar, like the Seventh, has undertaken.

But let me point out that we have been innovative as well as redundant. One of the remarkable developments of the past year or so, has been the discovery of the wealth of classification rationale to be found in myth and folklore. We have just begun to tap this resource in our studies of bears and pigs.

Consider the high technology revealed in the reports from the Grimm Brothers: the tablecloth that needs only to be spread to produce unlimited nourishment, the gun that never misses. The birds that exercise constant surveillance over the enemy. Then there is Mother Goose. Some years ago, there was published a delightful little book called *Mother Goose Censored*, showing what you could do with judicious deletion. I quote: "*There was a little girl who had a little curl* right in the middle of her *deleted.*"

When she was good, she was very very good; and when she was bad, she *deleted.*"

Or, "Peter Piper, Pumpkin Eater, had a wife and couldn't *delete* her."

"He put her in a pumpkin shell and there he *deleted* her very well."

Obviously, Mother Goose can provide useful training in the subtleties of paragraph marking. Now, I'm going to tell you a couple of stories I have gleaned from the public prints about the dilemmas of classification.

Classification meets its greatest challenge and is most vulnerable when the needs of the military clash with civilian needs. After the bombs dropped on Hiroshima and Nagasaki the U.S. Government in a burst of euphoric candor issued the Smyth Report. There are people in classification who continue to debate the widom of that release. (It made life more difficult for many of them.) But it started the ball rolling – a ball that did not stop 'till the technology of commerical fission reactors was completely in the public domain. It is what you might call a classic demonstration of what science, engineering, and industry can accomplish when the wraps of secrecy are lifted. For those who believe in progress as opposed to zero growth it is a magnificent demonstration, justifying the acceptance of the inevitable hazards.

It is ironic that the brightness of the new atomic age is now viewed by many as fire from hell. The genie is out of the bottle and we have no words to get him back in.

Lately we have seen glimpses of a new confrontation in the world of nuclear energy. This time it is fusion not fission. The invective has a familiar sound. On January 1, 1973, Sam Goudsmit, an atomic physicist of great reknown, made the following remarks in his New Year's editorial in *Physical Review Letters,* entitled "Secrecy Again".

> The new secret subject is fusion, more specifically laser-induced fusion. We don't know why it is secret. We have been told to mind our own business and not mingle in matters of government policy or politics. Our own business is publishing papers on advances in physics, and that is where we got into difficulties with secrecy.
>
> All we know about fusion is what we read in the newspapers and journals. It is heralded as the energy source which will solve all the world's problems. It is inexhaustible and pollution free. The remotest corners of the world will get enough energy so that everybody will be rich and can relax. Keeping work towards this goal secret sounds like hiding progress in cancer research. Perhaps it is done to prevent raising false hopes, or to prevent the premature sale of stock in oil companies. We don't know, and we don't understand.
>
> Recently, we received a Letter on the subject which was promptly sent to a referee. He prepared a long critical report, but could give us only two short paragraphs since the rest has to be declassified which will take a couple of months. We informed the author about the delay. He was not surprised and believes that the referee's critique most likely concerns items which the author had to omit from his Letter because of secrecy. Can physics advance in this way? Isn't it silly!
>
> Let us hope that the New Year will bring some enlightenment. We wish our readers, our authors, and especially our referees good luck in 1973 with ample support and successful research. S.A. Goudsmit

Next month the British journal *Nature* followed up with its own editorial on the subject and tied it to an article by Dr. Fred Winterberg published in the same issue. After a brief description of the article, which deals with what Winterberg refers to as microfission explosions, the editor goes on to say

> everybody will agree that calculations like these are at once interesting and stimulating and there is much to be said for making sure that they are published.
>
> This is why it is disturbing that in the past few months, there has grown up a cloud of officially inspired reticence about publication in the field in which Dr. Winterberg works. It is widely known that the use of lasers as a means of stimulating nuclear explosions, fission or fusion, has in the past few years before considered seriously by the United States Atomic Energy Commission and similar organizations elsewhere. That is as it should be. But the US Atomic Energy Commission (now ERDA as you know) is also exceedingly sensitive about the publication of results in this intriguing field and, to the extent that practical applications may be concerned, that too is proper. The trouble is that the passion for secrecy which is properly applicable to the potentially practical applications of these new technologies is, of course, entirely inappropriate where theoretical considerations are concerned, especially when their authors have no official connection with the Atomic Energy Commission. This is why it is a considerable scandal that there have recently been difficulties in refereeing articles submitted in good faith to journals, especially where the publications are American.

A glaring offense against seeming practice is described in *Physical Review Letters* (30,1; 1973) by an editor of that distinguished journal, Professor S. A. Goudsmit.

> This tale is not merely a description of a nonsense but a serious criticism of the way in which professional scientists conduct themselves. Is it really credible that serious professional people should write a scholarly opinion on a colleague's work and send this to the security men, not to the person for whom it is intended? Is it sensible, in any case, that the US Atomic Energy Commission should persist with a policy on classification which fails to distinguish between the kind of work were secrecy is legitimately applicable — where imminent practical applications are in question, for example — and the theoretical work or basic research typified by Dr. Winterberg's article? To pursue a policy like this is to recreate the frenzy of the 1950s. And because, where laser-induced fusion is concerned, the Atomic Energy Commission has apparently been trying to prevent independent authors from publishing their entirely independent research, is it not time that the scientific community said what it thinks of policies like these?

That same month the *Schweizerische Bauzeitung* heaped its own brand of scorn on the long-suffering AEC in an editorial entitled, *Energiekrise-Eine Folfe missbrauchter Geheimhaltung?* The energy crisis – is it a consequence of misused secrecy? I quote again –

> "Standing in the way of the most rapid... realization of these possibities that science and technology have revealed are hindrances both political and otherwise. Convenient secrecy determinations and falsely interpreted research priorities make it difficult or even imposible to achieve intellectual cross fertilization among scientists in this field and bring about effective communication among corresponding institutions – and not just those in the USA and USSR. So it happens that the East European editor of the IAEA technical journal *"Nuclear Fusion"* felt impelled by the intervention of the *American* Atomic Energy Commission to delete from its publication calendar an article related to this field because it was said to contain secret information. (Which raises the question whether the secrecy order represented no more than a legitimate security requirement and did not more likely serve the interests of economic monopoly.)"

Then referring to Goudsmit's editorial, our Swiss friend goes on to say,

> "Thus independent American inventors in this field are at the mercy of the weighty pressure of the USAEC and are forced as in other times and other fields to read between the lines."

The writer concludes by debating somewhat petulantly the wisdom of the Swiss Bundesrat in becoming the first partner in the nonproliferation treaty, particularly if the treaty should apply to microfusion reactors.

As a footnote I might add that in addition to mention in the *Schweizerische Bauzeitung,* Winterberg also got his thoughts published in the German journal *Laser + Elektro-Optik* under the title "Fission mit Laser?". If anybody profited by all this, I guess it was Fred. I hope he has a good sense of humor.

The most recent turmoil in this field has boiled up out of last year's visits to U.S. laboratories and conferences by the Soviet scientist L.I. Rudakov who is interested in using electron beams rather than laser beams to bring about microfusion. I understand his ideas were published last summer in the August 20 issue of the Soviet Physics Journal, *Journal of Experimental and Theoretical Physics, Letters.* The English-language version lags behind the Russian edition by a half year or more and the latest copy in our KMS Fusion library is August 5; so I can't tell you what Rudakov said. But I can tell you what Bill Metz said last October. Metz is on the editorial staff of *Science* (published by the American Association for the Advancement of Science) and covers research news.

> As a noted Russian scientist spoke about the latest advances in electron beam fusion last summer, "a number of mouths dropped open" at the three government laboratories where he spoke. The information he gave freely to an unrestricted audience was considered sensitive, by the American classification guidelines, and after he left, officials at each laboratory received phone calls from Washington urging them to keep the talk quiet and to remain noncommittal about the information and its importance. Just whom these measures would keep in the dark is a puzzle. The Soviets obviously knew about it, as did much of the American scientific community by the time the tour was finished. It seemed as if the system designed to keep American secrets from getting out was being applied to keep Soviet secrets from being broadcast.
>
> No American researcher says for attribution whether Rudakov's ideas are classified because the classification guidelines themselves are classified. What is, or is not secret is considered just as sensitive as the secrets themselves. Speaking for the Energy Research and Development Administration, which manages all nuclear weapons research, L. E. Killion said Rudakov's design appears to be "a novel idea and we are going to look at it," When asked if it were classified, he said, "I was not there and would not want to comment on other details."
>
> Apparently a brilliant idea underlies Rudakov's fusion pellet design and so considerable scientific prestige will go to those credited with it. Part of the ERDA policy of keeping mum may be motivated by embarrassment that the Soviets have taken credit first. If so, it is likely the American classification guidelines will soon be relaxed.
>
> In July 1973, Rudakov talked about an explicit pellet design at a European fusion meeting, and within a year some related American work was declassified.
>
> Whatever the reason for official silence, it is hardly motivated by the urgency of keeping secrets from the Soviets. In this instance, the information has been flowing the other way. – William D. Metz

One sometimes suspects that Bill Metz is a frustrated Jack Anderson trapped in the sober halls of science.

Echoes of the affair have shown up in odd places like the St. Paul *Sunday Pioneer Press* which in March copied a piece written for *NEWSDAY* by Ernest Volkman that started off by telling its readers:

> "WASHINGTON – U.S. officials have put strict security wraps over a lecture by leading Russian physicist – including seizure of the blackboard on which he wrote equations – given to an audience of American scientists that revealed significant Soviet breakthroughs in top-secret fusion research, U.S. Intelligence sources say.
>
> The physicist's revelations, which came during a talk last summer at a leading U.S. nuclear weapons research laboratory, astonished his scientific audience because, the sources say, they showed what appeared to be great advances in thermonuclear fusion by the Soviets.
>
> According to Pentagon experts, the disclosures caused concern that the Soviets are nearing a breakthrough in developing thermonuclear weapons 100 times more powerful than the largest current weapon.
>
> According to one source, 'mouths dropped open all over the room' as nearly 100 American scientists listened, for Rudakov was outlining top-secret developments in the Soviet program and revealing the direction of future Soviet thermonuclear weapons designs.
>
> Immediately after his talk, sources said, security officials advised the Americans in the audience that the talk was classified, including Rudakov's blackboard notations, and seized the blackboard."

I find the picture of a 100 slack-jawed scientists gazing in consternation at an impounded blackboard utterly fascinating. You have noted, I am sure, that among journalists all disclosures are top secret. It reminds me of the time back in Oak Ridge when I came to work one morning and found a picture of Uncle Sam pointing an accusing finger and saying I had endangered my country's security by leaving a top secret document on my desk the previous evening. Even though I knew I had no TS documents, it gave me a bit of a turn. You know the feeling. It turned out that the guard had picked up a newspaper account of a meeting at AEC in which machine-tool manufacturers had been briefed on the coming needs for ultraclose tolerances. Six columns wide the headline screamed TOP TOLERANCES TOP SECRET. Then I understood what the security people were looking for when they said you don't want too much intelligence in the guard force.

The hue and cry over Rudakov became a shrill crescendo when the Fusion Energy Foundation got hold of the study: F.E.F. is an offshoot of the American Labor Party, a marxist outfit that pushes for a strong energy development program, particularly fusion, presumably on the theory that a socialist state can succeed only in a highly developed, energy-rich economy. Often they sound like conservative Republicans; but they appear to view all history – particularly contemporary history – in terms of conspiracy, and their rhetoric frequently resembles the rhetoric of Chinese wall posters.

Here is a sample, called "The wrecking of Plasma Physics".

> "More significantly, none of the ERDA officials would admit to the scientific significance of Rudakov's work. This demonstrates that even if ERDA wanted to administer a crash development program in fusion research – essential for realization of the new world economic order – they would not know how to go about it .... But the possibilities for full theoretical and experimental investigation of these basic physical processes will remain blocked as long as the vampires such as "Dracula" Teller who sucked the blood out of science during Rockefeller's destruction of nuclear physicist J. Robert Oppenheimer remain in control."

Those who work in classification have to get used to vituperation. It is not as bad as being in the CIA or FBI, but we are all victims of the distorted mentality so prevalent in the sixties that looks on the business of upholding and defending our country as obscene, particularly if it involves secrecy.

There seems to be a lot of people who don't trust Prestone – I mean *Classification*. But when you look at the alternatives to trusting classification, things get a bit scary – in spite of what "Dracula" Teller keeps arguing. The stories I have told you are but two examples of the storms, familiar to all of us, that are always swirling around our heads. It is not only Woodbridge who is in disgrace with fortune and men's eyes, beweeping his outcast state. There is little recognition of the lonely plight of those who stand at the last ramparts or – to switch the metaphor – keep a finger in the dike, never quite sure that there is a battle to be won or a flood to hold back. It is the state of affairs that is redundant, tautological, and once more redundant – and does it call for patience!

So there you are. If you ask me what I think about Rudakov and Rockefeller and the rest, I have to say that I don't know. My badge says *ESCORT REQUIRED.*

PART TWO

SELECTED PAPERS

1977

ANNUAL MEETING – 1977

Dean C. Richardson
President

Welcome to Washington and to our Thirteenth Annual Seminar. Before I call the business meeting to order, I would like to introduce **Dave Sims,** Security Manager for IDA, who will speak for the American Society for Industrial Security.

MR. DAVID SIMS: Thank you, Dean. Good morning, ladies and gentlemen. I am not a member of NCMS, but your business is one of my responsibilities, and I follow your progress with great interest. I am particularly impressed by the fact that while you have fewer members than ASIS, you seem to be much more deeply involved in informational and liaison activities, with Congressional committees and other governmental agencies, and if proof of this were needed, we have only to look at your program for the day. I think this is most important and I would like to see ASIS get more involved along similar lines.

I have been asked to read the following letter.

> "To the President and members, the National Classification Management Society, on behalf of the American Society for Industrial Security, most sincere professional and personal best wishes, for a most successful Thirteenth Annual Seminar of the National Classification Management Society.
>
> "We have received much of value from our communications and other exchanges with NCMS again this year. We firmly believe continued professional contact with your Society will enhance and assure greater success in the advancement of security, both nationally and internationally."
>
> Wayne L. Hall
> President
> American Society for Industrial Security

While I have the opportunity, Wayne has asked me to say a few words on a subject that we think is very important to members of NCMS and ASIS, as well as people who have not had the good sense to join one of our organizations. At long last, the ASIS Professional Certification Board is a reality, and I am not going to explain at length what it is; basically the Certification Board is going to recognize by certifying as professionals, those people in the security business who have achieved professional standings.

Membership in ASIS, while certainly desirable from our point of view, is not a requirement to certification. The basic requirement will be ten years of security experience in positions having responsibility for independent decisions and actions. There will also be qualifying combinations of experience and education, with the experience requirement decreasing as the educational level rises.

In addition to meeting experience and/or educational requirements, candidates must also pass a series of eight tests, four of which will be mandatory subjects and the other four chosen by the candidate himself, from among a group of sixteen subjects. For your information, the four mandatory ones will be Security Management, Physical Security, the Legal Aspects of Security, and Investigations. The other sixteen subjects will run the gamut of security special areas, such as educational institutions, retail, hospitals, and so forth.

Now from the first of August, 1977 to the first of January, 1978 and only during that period - - I want to emphasize *only* during that period - - the professional certification board will accept applications from those with five years of additional experience in responsible charge, in lieu of taking the test.

Then on a different point our Executive Director, Perry Norton, has asked that I invite attention to the brochures for the ASIS 23rd National Seminar. They will be on your registration table. We cordially invite you to attend and would welcome your participation.

Thank you for the opportunity to participate and I add my best wishes to those of Wayne Hall and the Board of Directors of ASIS, for a most successful Thirteenth Seminar.

PRESIDENT RICHARDSON: In connection with the ASIS 23d Seminar mentioned, I have the honor and pleasure to announce that the Society has been invited to participate. The letter of invitation I quote in part. "Mr. Dean Richardson, President, NCMS. On behalf of the Executive Committee 23rd Annual Seminar of the American Society for Industrial Security, the National Classification Management Society is invited to participate in our program by presenting a Classification Management Workshop. We have set aside the period from 1:45 to 3:00 P.M. and from 4:00 P.M. to 5:30 P.M. on Wednesday, September 7 . . . "

The Board of Directors has voted unanimously to accept the invitation and I hope to see many of you in Orlando in September.

Moving to our annual meeting, the first order of business is to announce those elected to fill the three vacancies on the Board of Directors. I call on Joe Care, Chairman of the Nominating Committee to announce the results.

MR. JOSEPH C. CARE: We ran the election to fill impending vacancies on the National Board of Directors from New London, Connecticut in accordance with the Bylaws of the Society. Those elected were Fred Daigle, Jack Robinson and Eugene Suto. There were 152 ballots cast, 58% of the membership participated.

PRESIDENT RICHARDSON: Thank you for your efforts, and those of Clarissa DeAngelis. For those of you who may not fully appreciate the difficulties, serving on the Nominating Committee is not an easy task but is a most important one for the Society. Congratulations to those elected.

Next, I would like to introduce Elaine Gruber. Elaine is the editor for the 1976 Seminar Journal, which is in process right now, and will be out as soon as possible.

Then, I would like to announce our Chapter Chairmen and Area Coordinators and recognize those who are here. Joe Care for the New England Area. John Jernigan from Mid-Atlantic. John is not here today. Frank Larsen from Washington. Jim Buckland from the Southeast Area. Bob English from the East and North Central Area. I might comment that Bob is moving to Washington. Bill DuCoing from the Southwest Area and the new Dallas Chapter is not here. Bill Six, Southern California Chapter. And Elmer Anderson from the Northern California Chapter.

Gentlemen, would you like to give a short summary of what you have been doing this year. Let's start with Elmer Anderson, Chairman of the Northern California Chapter.

ELMER ANDERSON: We have a program scheduled for the 23rd of June, a workshop at 4:00 P.M. and a speaker. The speaker will cover the Export Program and the workshop will be on the topic of Foreign Visitors. We have meetings planned through the year. In addition, we are soliciting for new members. We provided potential members with the article on retention from the *Bulletin* and have sent subsequent articles as well. Our results are that as of the end of last year, we had increased to 31 members, and we anticipate having at least 50 members by the end of this year.

PRESIDENT RICHARDSON: Bill Six, what are your views from Southern California?

MR. WILLIAM SIX: Southern California has continued to maintain an active program. We have run from 50 to 100 participants at each meeting. I may report that Vern Lusk has been elected as Chapter Chairman for the coming year.

PRESIDENT RICHARDSON: Bob English, what about the East and North Central Area. This is a difficult one because you don't have Chapter Meetings, but you might have a few things to report.

MR. ROBERT ENGLISH: We haven't had too much. We have lost a number of members just through retirement. The distances involved are such that we just haven't been able to get together. It is difficult to achieve a "group" in that area.

PRESIDENT RICHARDSON: Jim Buckland, Southeast Area; Have you got anything to report?

MR. JAMES BUCKLAND: An important event in the Southeast Area was the Mini-seminar we had down in Panama City in the Spring of 1976 which the Naval Coastal Systems Laboratory hosted. I would like to introduce Marilyn Griffin for those of you who don't know her. She and her boss ran an absolutely outstanding little seminar, and she personally deserves a lot of credit for it.

PRESIDENT RICHARDSON: Jim Morgan, from the Southwest Region, and we have a Chapter now. We have been in business for a little while. Jim, would you stand and say a few words.

MR. JIM MORGAN: We are starting from scratch. It is hard, but we do have 12 active members and we have 12 more prospective members. We are working on a repetitive basis. We have been organized about a year and a half. At our last meeting, B. K. Bradfield from G. D. presented the Trials and Tribulations of Arranging Business in Foreign Nations, along with their program and the F-16 Program. I think most important, we look forward to seeing you all next year now in Dallas; under Dean's leadership, we hope to have an excellent program and as you notice, we are sponsors to the yellow rose of Texas.

PRESIDENT RICHARDSON: Frank. Washington D. C.

MR. FRANK LARSEN: As you might suspect, the Washington Chapter suffers a bit in terms of a more rapid turnover than perhaps some of the rest of you, but nevertheless the membership has increased by some 15% this past year. One of the things we have established with the help of Mr. Norton (EXECUTIVE DIRECTOR OF ASIS), is a direct Liaison with the Washington Chapter of ASIS. We feel that there is a very fertile field for broadening the base of our own efforts, not only in terms of interesting people who are unaware of NCMS, that do belong to ASIS, but also, through the good offices of the national headquarters of ASIS, utilizing their facilities for promoting some of the things that NCMS believes in.

As you know, Perry is a member of our Society, and feels that both Societies can benefit in areas of mutual interest, and that there is no point in re-inventing the wheel too frequently. So I suggest that those of you who, in other parts of the country have ASIS Chapters, think about a joint meeting and I think you will find them beneficial.

We are looking forward to a meeting before summer, yet to be announced, at which time we will have a new election of officers.

PRESIDENT RICHARDSON: Thank you, Frank. Joe Care, you got away awfully easy this morning, with your short speech. Would you like to say a few words about the New England Chapter?

MR. CARE: I want to thank all of you who came to Connecticut last fall to our Mini-Seminar; staff, and all the attendees, Frank Larsen, Dean Richardson. In fact, the walls of the Ramada back in Mystic are still echoing with the eloquence and intellect of Mr. Woodbridge. We are looking forward to running another one sometime in the future.

PRESIDENT RICHARDSON: Thank you, Chapter Chairmen. I want to add a congratulatory note to each one of these Chapter Chairmen. Not one of them knew I was going to call on them to speak. How is that for extemporaneous speaking?

Thank you, gentlemen, for your support, and we look forward to lots more support this next year. And now Vice President Dick Butala will report to us on the membership.

MR. RICHARD G. BUTALA: Good morning, ladies and gentlemen. Maybe most of you noticed in our *Bulletins*, and maybe some letters I have been sending out, that I have been trying to get more people to join our Society. I get a little frustrated when I look at ASIS' multi-thousand membership and then look at our relatively small number. However, I just look back and say, well we are in a little different field and we have a specialized area. *But*, there are a lot of people out there that should be members.

In trying to identify these people, I have had some help from Gene Suto, Frank Larsen, in providing me a list, a contact list, of people in the Department of Defense, ERDA, NASA. I have been personally contacting these people in the last six months, with letters and applications; trying to get them to join us. We have had some success, in the last three months, we have some 12 to 13 new members as a result of this writing campaign.

It appears to me that the most effective means of getting our new members is the mini-seminar (of which there have been three) that we have been holding in different parts of the country. We have contacted those who have attended the seminars individually and about 13 of them have joined. In short, we have had a pretty good year for new members - - now let's keep them.

A little breakdown, since last year's seminar in San Diego, we have had 56 new members. That is as of today. We received two applications today, in fact.

You will be interested in our population by Chapter/Area.

New England Chapter	17 members
Mid-Atlantic Chapter	23 members
Washington Chapter	87 members
Southeast Region	17 members
East-North Central Region	16 members
West-North Central Region	6 members
Dallas Chapter	10 members
South Central Region	2 members
Southern California Chapter	64 members
Northern California Chapter	33 members

Again, our goal for membership is to have as members those people who work or have interest in our subject matter; both industry and government. Then when we have meetings or seminars such as this we can meet, exchange ideas and discuss problems. Further, when we have a problem, we can telephone an individual, government or industry, and likely solve the problem without difficulty. Your membership book is a valuable tool.

PRESIDENT RICHARDSON: Thank you, Dick. At this time our Treasurer, Alan Thompson, will report on our financial posture.

MR. E. ALAN THOMPSON: One of the real advantages of having a seminar in May as against in July, is our books look better. They look better, because at the beginning of the year you have receipts from current dues and you haven't spent all of them *yet.*

So our financial posture is about as follows: Total receipts as of this date from 1 January 1977 are $4,829.71; Disbursements to date have been $3,301.59 for a net receipt over disbursement of $1,528.12. The net worth of the Society is $15,898.54.

Our financial picture looks attractive but the big bills are ahead of us. And, as we look at our budget, I must report that there will be some net outflow from savings. We expect that the reduction in net worth will be modest, but it remains to be seen what costs will be; it is difficult in May to know what our financial situation will be in December.

PRESIDENT RICHARDSON: Is there any other business to be brought before this Society? Any Old Business that we have left out? Any New Business that anyone would like to bring up?

Very well, let me summarize. This ends the Society's 1976/77 year. We have had a short year but a good year, and we have made progress. Our membership is at 272 compared with 220 at Seminar time last year. Our *Bulletin* is back on schedule. We have had several *Letters to the Editor* of which I hope there will be more from all of you. The Anniversary Journal has been completed at long last and you will find it a valuable tool.

We have held two regional "mini-seminars"; one with the New England Chapter, one with the Northern California Chapter. We have had more audience participation in our regional seminars and in our national seminars. We were invited to make a formal presentation on careers in information security and classification management at the Annual Interagency Classification Review Committee Symposium, as you know from our reporting in the *Bulletin*. We were honored to be invited to this all government symposium.

Then, to expand our horizons, we began our Annual essay contest. It netted only six people who dared to share their views with the Society. I urge you, all of you here to share your views with us. It's a means by which you can express views on operations or problems, make recommendations or whatever, that might improve the program and provide the Society and your Board with points that might form the basis for a position paper. *Submit an essay for next year's contest!*

Last but not least, we have a commitment from the Dallas Chapter to hold the Fourteenth National Seminar in Dallas on May 16, 17 and 18, 1978. This will be the first time the Society has held a National Seminar in other than California or Washington, D.C. Plan now to attend.

That completes my summary of the Society's activities while I have had the honor to be your President. I appreciate your support and urge that you continue it an expand it for the coming year. In closing I announce the Officers elected to serve you for the coming year.

Fred Daigle	Secretary
Alan Thompson	Treasurer
Dick Butala	Vice President
Jim Buckland	President

WHO SHOULD CONTROL SECRECY?

Frederick J. Daigle
Lockheed Missiles & Space Company

Presented to Commonwealth Club of California
May 1976

On the sixth of May, past president Daigle was invited to present a talk to the Commonwealth Club of California on the topic of the status of legal and regulatory bases for classification. The occasion was the kick-off of a study by the National Defense Study Section of the Club chaired by RADM Henry J. Armstrong (USN-Ret.). A not small amount of effort was required, as you might imagine, and it seemed appropriate that the product be made available to our members. The study is underway under the title "Who should Control Secrecy in Regard to National Defense and to What Extent? Fred has been asked to advise on certain of the aspects relating to his presentation. The presentation follows:

To assist you in understanding my frame of reference to various terms, I will define those that can be considered similar or the same depending on your personal exposure to security.

Classification Management: Understanding of the philosophies, doctrines, standards and criteria of the government's programs for identifying and designating information that requires protection in the interest of national defense or national security.

Security: The determination and application of appropriate security measures to information that is identified and designated as requiring protection – in other words information that is classified. Classification determines what information is classified, identifies the vehicle that contains that classified information and security protects it through marking, control of access to the information and control of access to areas where the information is available.

Classified Information: Variously defined over the years as information of great importance to keep from an enemy – then national defense information and now national security information.

Executive Order: An order signed by the President on any given subject, that becomes effective upon his signature and subsequent publication in the Federal Register. It has the effect of a regulation, but has no status or being in law. Violation thereof could be punished by job loss at best.

The need to protect information from disclosure to others has been with us forever. I personally regard it as one of the basic decisions of the Almighty, after He made man and then woman. When He placed Adam and Eve in the Garden of Eden, He must have decided that the physical characteristics of each would be classified. Having no professional security force at hand, He devised the simple fig leaf as the protecting device. We all know how long it took to penetrate (if you will pardon the term) that device, and as a result, there was no longer a need to classify; the only two people from whom information was being witheld, gained access; there was no one except the Big Boss to whom to report the fact of compromise, and He already knew; ergo, end of that classification and security system.

It has continued in this vein ever since, once the information you want to protect from someone else becomes common knowledge, there should no longer be a need for security. But what about punishment for this failure to observe the classification of information and violation of the security procedures. God was not encumbered by Executive Orders, or by Statutes so He simply applied His own punishment. Without benefit of the judiciary to question His right to punish, He simply banished Adam and Eve from the Garden of Eden. Put yourself in their place today. How long do you feel it would take the President of the United States to impose a lasting punishment if you were to violate his Executive Order as to what was classified and what was not? Look at Ellsberg – he never was convicted or punished, however he freely admitted thwarting the provisions of Executive Order 10501.

How have we as a nation gotten into this position?

From the earliest days of our Republic, the President, in carrying out the provisions of Article II, Section 2, of the Constitution as the Commander in Chief, has limited the dissemination of information affecting our defense and foreign policy interests.

The first instance of the use of Article II authority to effect secrecy was in 1790 when President Washington presented to the Senate for its approval a secret article to be inserted into a treaty with the Creek Indians. One authority on the history of classification markings has traced such labels as "Secret," "Confidential," or "Private" on communications from military, naval, or other public officials back almost continuously for more than a century.

Thus, the historical review of the confidential treatment of certain defense and foreign policy records and documents shows that, to some degree, secrecy in military and diplomatic affairs has always been practiced by the Executive Branch, although a formal classification system to protect such types of information did not develop until more recent times.

The origins of the present security classification system can be traced just prior to the World War I period. On February 16, 1912, a general order was issued by the War Department that established a system for protecting information relating to submarine mine projects, land defense plans, maps and charts showing locations of defense elements and the character of the armament, and data on the number of guns and supply ammunition. The order, however, prescribed no particular security markings.

More than 5 years later, after the United States had entered the war, the General Headquarters of the American Expeditionary Forces published General Orders No. 64 establishing the classifications of "Confidential," "Secret," and "For Official Circulation Only." Limitations on reproduction and distribution were also provided. The system was patterned after British and French procedures.

Soon thereafter, the War Department issued more precise definitions of "Secret," "Confidential," and "For Official Use Only." Citations were also made in the Order to punish for failure to protect such information under provisions of the articles of war or under Section 1, Title 1 of the Espionage Act, which had become law on June 15, 1917.

We may surmise that invocation of the Espionage

Act of 1917 was considered advisable because so many officers of the war-time Army were drawn from civilian life and therefore would not have the instincts of professionals.

There is no indication that there was any realization at this time that difficulties could arise in enforcing the Espionage Act if official information relating to the national defense was not marked as such, insofar as it was intended to be protected from unauthorized dissemination.

The Navy Department issued their General Order in 1918 establishing and describing three "classes of correspondence and information" – "Secret," "Confidential" and "Nonconfidential."

Several years after the end of World War I, the security classification system was formally continued by Army regulation and three levels of classification markings were described: Secret, Confidential, and For Official Use Only.

The Secret definition was "information of great importance and when the safeguarding of that information from actual or potential enemies is of prime necessity."

A noteworthy fact is that these regulations failed to relate to the provisions of the Espionage Act of 1917 or to limit their application to defense information.

A subsequent revision of the regulation in 1935 added the term "Restricted," to be marked as follows:

> Restricted: Notice – this document contains information affecting the national defense of the United States within the meaning of the Espionage Act (50 USC 31,32). The transmission of this document or the revelation of its contents in any manner to any unauthorized person is prohibited.

A February 11, 1936, revision of Army Regulations 330-5 dropped the marking "For Official Use Only" and redefined "Secret," "Confidential," and "Restricted" to bring them more into line with similar Navy regulations. It defined Secret as:

> "Information of such nature that its disclosure might endanger the national security or cause serious injury to the interests or prestige of the nation, an individual, or any government activity, or be of great advantage to a foreign nation."

Note, this is the first reference to national security, and it extended the applicability of protective markings to "Nondefense" Information. The 1936 revision of Army Regulations 330-5 contrasted with earlier versions of the same regulations, which had evaded facing up to this question of applicability. On what basis the regulations were now given their extended applicability is not made plain. The effect was to apply the menace of prosecution under the Espionage Act to the protection of whatever defense or "nondefense" information War Department officials might want to protect. Note that so far none of these restrictions have been laws, only directives to the military.

The first use of an Executive Order in the security classification field took place in 1940, when President Roosevelt issued an order entitled "Defining Certain Vital Military and Naval Installations and Equipment." As authority, he cited the Act of January 12, 1938 which stated:

> Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installation or equipment without first obtaining permission of the commanding officer.

Violation of the law was subject to criminal action, a $1,000 fine and/or imprisonment of up to 1 year.

In defining the installations or equipment requiring protection, the President listed as a criterion the classification as "Secret," "Confidential," or "Restricted" under the direction of either the Secretary of War or the Secretary of the Navy. In addition to military or naval installations, weapons, and equipment so classified or marked, included in the definition were:

> All official military or naval books, pamphlets, documents, reports, maps, charts, plans, designs, models, drawings, photographs, contracts, or specifications, which are now marked under the authority or at the direction of the Secretary of War or the Secretary of the Navy as "Secret," "Confidential," or "Restricted," and all such articles or equipment which may hereafter be so marked with the approval or at the direction of the President.

In his study of Executive Order 8381 and Public Law 418, Archivist-Historian Irvine makes these comments on the legislative history of the Act.

> Congress, in passing the Espionage Act of January 12, 1938, can hardly have expected that it would be interpreted to be applicable to documentary materials such as "equipment." The provisions of the Executive Order were probably a substitute for equivalent express provisions of law that Congress could not be expected to enact. Mention may be made in this connection of the refusal of Congress, long after the attack on Pearl Harbor, to pass the proposed War Security Act submitted to Congress by Attorney General Francis Biddle on October 17, 1942.

A government-wide regulation dealing with security classification was issued in September 1942, by the Office of War Information under authority vested by Executive Orders 9103 and 9182. This provided definitions of classified information – "Secret," "Confidential," and "Restricted" – and designated authority to classify. It also contained provisions warning against over-classification and provided instructions for the identification of classified information, for its proper dissemination, and proper handling. These Executive Orders also referred to information endangering "National Security."

The National Security Act in 1947 created the National Security Council (NSC), the NSC was given responsibility to consider and study security matters, which involve many executive departments and agencies, and to make recommendations to the President in this vital area.

The 1940 Executive Order was superseded in 1950 by President Truman's Executive Order 10104, "Definitions of Vital Military and Naval Installations and Equipment," the new Order continued authorization for

the same three classification markings as in the previous Order and formalized the designation "Top Secret," which had been added to military regulations during the latter part of World War II to coincide with classification levels of our Allies. The Order gave the Secretary of Defense and the Secretaries of the Army, Navy and Air Force the authority to classify or direct to be classified the types of information described in the Order.

It is important to emphasize that through the historical period of the use of classification markings described thus far until 1950, such formal directives, regulations, or Executive Orders applied to the protection of military secrets, rarely extending into either those affecting non-military agencies or those involving foreign policy or diplomatic relations. One exception is in the area of communications secrecy, governed by Section 798 of the Espionage Act. This law, which protects cryptographic systems, communications intelligence information, and similar matters, applies, of course, to both military and non-military federal agencies such as the State Department.

On September 24, 1951, President Truman issued a new Executive Order formalizing and extending the security classification system within non-military agencies as well as the defense establishment. The Order, entitled "Prescribing Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information which Requires Safeguarding in the interest of the security of the United States."

It permitted any executive department or agency to classify information on a uniform basis and defined "Classified Security Information" to mean "Official information the safeguarding of which is necessary in the interest of national security, and which is classified for such purposes by appropriate classifying authority."

The order was strongly critized by some segments of the press for its vagueness and potential abuses it made possible and also by a number of members of Congress. A Bill (S.2190) was introduced in 1951, to "prohibit unreasonable suppression of information by the executive branch of the government," which, in effect, would have repealed the Executive Order. No action was taken on the measure.

Remember – as we progress – the lack of Congressional action!

When President Eisenhower took office in January 1953, he took notice of the widespread criticism of Executive Order 10290 and replaced the controversial Truman Order with Executive Order No. 10501, "Safeguarding Official Information in the Interests of the Defense of the United States." This Order became effective on December 15, 1953; it was amended several times in the succeeding years, but for almost 20 years served as the basis for the security classification system until it was superseded in March 1972 (by Executive Order 11652).

Executive Order No. 10501 reduced the number of agencies authorized to classify information, eliminated the "Restricted" category, and redefined the usage of the three classification markings authorized:

> Official information which requires protection in the interests of *National Defense* (Note: not national security) shall be limited to three categories of classification which in descending order of importance shall carry one of the following designations: Top Secret, Secret, or Confidential. No other designation shall be used to classify defense information, including military information, as requiring protection in the interests of national defense, except as expressly provided by statute.

After the publication of EO 10501 many official and unofficial happenings were taking place, especially during the last ten years of its effective life. Civilians in government and in industry, plus many military persons who dealt in security were, as individuals, becoming more unrestful with the EO and its ramifications. The Atomic Energy Act of 1954 was the first modern law to define information that required security protection and provided a basis in law, by statute, for this protection. It further provided punishment for offenders and established an agency to monitor the administration of these requirements – The Atomic Energy Commission. The Commission interpreted the law, issued regulations for compliance and preferred charges against individuals or companies that failed to comply with the law.

An outgrowth of this commission activity, was the establishment of the concept of classification management. To identify and manage the classification of information thereby permitting security procedures to be defined and enforced. Further outgrowth was the unrest of the classification management cadre in the AEC when they realized that all the interpretation was downwards and not across or upwards, so they met to form a group to discuss problems and exchange ideas. The companion industries involved in nuclear energy declared their interest and participated, this soon extended to all industry, especially aerospace, that felt the concept could even better serve those classification requirements handed down by the military without the benefit of law or a single source of interpretation. A professional society was organized and was chartered in 1964 by the state of New Mexico and became the National Classification Management Society. This society is still active today in examining the Executive Orders and their interpretations as published by the various government agencies.

In 1972 President Nixon observed the unrest in the nation and in the Congress over the inadequacies of Executive Order 10501. Several bills had been introduced in the House and the Senate in an attempt to astablish what might be called a National Secrecy Act, all of which failed to grasp the enormity of the situation, so failed to gain substantial support.

During this period two major committees were addressing themselves to the problems of secrecy in government. One was the House Foreign Operations and Government Information Subcommittee under the guidance of Chairman William S. Moorhead, Pennsylvania, which is now known as the Abzug Committee; and the Senate Committee on Government Operations Subcommittee on Intergovernmental Relations chaired by Edmund S. Muskie, Maine. Both of these committees held extensive hearings into executive and other government secrecy, and published voluminous reports on their activities. While this was going on and after the eruption of the controversy over the publication of the Pentagon Papers excerpts by the *New York Times, et al.*, it was revealed that President Nixon had on January 15, 1971,

directed that a review be made of the security classification procedures in effect, and established an interagency committee to study the existing system, and make recommendations. These were incorporated into a draft revision to the Executive Order and circulated in January 1972 by the National Security Council for comment by key departments and agencies concerned with the security classification system. It is interesting to note here that a request to the White House Counsel for a copy of a draft for informal study and comment from Representative Moorhead was denied. Without any input from either the House or the Senate Subcommittees the revised version of the National Security Council draft was issued by Nixon on March 8, 1972, as Executive Order 11652 to be effective June 1, 1972. The implementation of this Order substantiated the same three classification levels; decreased the number of persons who could make original classification decisions (however, ignoring the fact that the thousands of us still would be required to make interpretive classification decisions); established an Interagency Classification Review Committee; in general alienated the United States Congress – Mr. Moorhead deplored its issuance as premature during a presentation on the floor of the House; and, further thoroughly confused the citizens of the United States who had to implement the various agency interpretations of the requirements. In all, it did nothing new for classification except to give recognition to the term.

The same three classifications exist, the Executive Order still appears to have for its basis in law the provisions of Article II of the Constitution. Even though Executive Order 11652 appears to claim a basis under the Freedom of Information Act (5 USC 552), it further is accused of confusing the sanctions of the Criminal Code that apply to the wrongful disclosure of classified information. This was further verified in an exchange between Assistant Attorney General Erickson and Representative Moorhead. After several exchanges Moorhead asked, and I quote, "This Executive Order just as the previous 10501, does not in and of itself create a law, a violation of which is a criminal offense?" Erickson: "That is correct." Moorhead summarized: "Mere disclosure of classified information, without the required intent under the criminal laws is not in and of itself a criminal violation."

Let's very briefly then compare what we in the United States have under the Executive Order system with what the British, for instance, have under their Secrecy Act. There have been many comments about the Secrecy Act and several recommendations that we adopt such a law in the United States. The Act is not a single law at all. Properly stated, it is "The British Official Secrecy Acts 1911 to 1939." The law is found in the laws of England which is the closest approximation to our U. S. Code. Many topics are covered in the law as they are in our Title 18, U. S. Code. But for simplification we will address only those that appear to approximate classification and wrongful release of classified information; effect of communication with foreign agents; wrongful retention, etc., of official documents; and wrongful receipt of official documents. With the latter – wrongful receipt – it became an offense under the Act for a person to receive prohibited information, just as it was for a person to pass such information, unless the receiver could prove that the receipt was contrary to his desires. No changes have been made to the 1939 revision to the Act. However, the provisions covering production and use of atomic energy were added in 1946. In this country the first use of the acts of this type was an Espionage Act passed in 1911. Although not common knowledge, it was drawn from the British Act of 1889 and was in fact intended, as substantiated by review of the Congressional record, to be an Official Secrets Act. This Act was superseded by the Espionage Act of 1917 which is still effective. Unfortunately the Act provides only for obtaining national defense information to which not entitled and for communicating this denied information to a foreign government or agent or employee thereof. It does not make it unlawful to communicate to other U. S. citizens nor for anyone to receive such information.

I have herein tried to relate to you some background on the evolution of classification in the U. S. Where are we now?

- We are operating under another in a seemingly endless series of Executive Orders which establish the various levels of classification and their markings intended for identification of information which is, quote, "in the interest of the national defense or foreign relations of the United States (hereinafter collectively termed national security) when applied to the protection of official information."
- It is the general consensus of opinion, by the judiciary and the legislative branches of the government that these Executive Orders are without a base in law or statute, and therefore violations thereof are not punishable under Title 18 U. S. Code which is our punitive code.
- Many major congressional attempts have been made over the years to provide a basis in law for protection of information marked with a classification identification; however none have been successful. There has always been congressional opposition to such an action prompted by heavy public opinion mostly from single interest groups. But mostly because Congress cannot agree on the *"how."*

Who should control secrecy in regard to national defense and to what extent? You recognize that question, as it is the basis for your current study project. The 94th Congress Senate Bill No. One, (S-1) which has been in committee since January 15, 1975, and has continued to receive unfavorable press, is in fact a rewrite of Title 18 USC, and in Section 1124 makes it criminal to disclose classified information to an unauthorized person, but not to receive it. It would for the first time recognize and substantiate an Executive Order on the subject. Permit me to read to you the recommendations of the National Classification Management Society, formulated during the year I was national President:

> The National Classification Management Society recommends the enactment of legislation that:
>
> Recognizes the need to protect certain information variously identified as national security information, national defense information, or information requiring protection in the interests of national defense

and foreign policy; and

Provides a statutory basis for such protection.

Further, the Society recommends that such legislation be consistent with congressional oversight responsibilities, but not deal in details of managing the classification system.

It is, in my opinion, altogether fitting that you address this problem at this time. It is obvious to me, based on reports from knowledgeable Washington people that S-1 will die with the 94th Congress as similar bills died with the 92nd and 93rd, due to the press of the election year, the inadequacies of the bill and a partial reluctance to allow the courts to rule on secrecy and establish case precedences. The alternative could, of course, be a National Secrecy Act. But, one must wonder if such a drastic measure is within the capabilities of the Congress to enact what with the new morality, the new freedoms for individuals and the new international relationships such as SALT and other treaties where it seems that our trend is to release secrets rather than protect them from anyone except each other. There is time to amend this trend and the 95th Congress could well be the vehicle but only if national security regains public popularity. We as individuals must do all we can to make this a reality.

Let me quote you Guy Wright, *San Francisco Examiner,* Monday, 5 April 1976, as an example of national attitude:

> "There are 15,644 federal bureaucrats who can stamp documents classified, which means the national security would somehow be endangered if ordinary citizens like you and me saw them.
>
> "The salary for that legion of secrecy freaks comes to $750 million a year, and their mountain of classified documents is growing at the rate of 3,600,000 a year.
>
> "It is rare enough for two people to keep a secret. The idea that 15,644 people can keep more than 3 million secrets is a psychopathic joke, and if the people in charge of this country don't know that, they are the wrong people to be in charge.
>
> "Most of this marathon stamp act serves no other purpose than to cover up some bureaucrats mistake, you can bet on it.
>
> "Yet Congress is considering a bill that would make it a prison offense for any government employee to tell a newsman anything that is on those 3,600,000 pieces of paper. And if the newsman printed it, he could be thrown in prison too.
>
> "Edmund Burke said, "Bad laws are the worst form of tyranny." This one sure fits that description.
>
> "My own unclassified suggestion to everyone in Washington from the man in the White House down: Take your SB-1 and stuff it."

I feel we need a National Secrecy Act, one that finitely defines national defense information and/or diplomatic information and makes the giving to unauthorized persons or receiving by these unauthorized persons including the 4th estate punishable under law.

I wish you the best in your study effort and offer my reference material and assistance and that of NCMS. Whatever your position, it will be eagerly received by the Congress, the ICRC of the NSC and by individuals in the Department of Defense.

SOME BACKGROUND NOTES RELATING TO SECRECY LEGISLATION

Jack Robinson
Center for Naval Analyses

Presented to the Commonwealth Club of California
July 1976

Introduction

I am honored to be invited to share with you some views that may, one hopes, add perspective and information to assist in the study of your topic "Who Should Control Secrecy and to What Extent." The substance of your topic is one that has been a matter of concern to the Center for Naval Analyses for which I work and to the National Classification Management Society of which I am the most immediate Past President.

My colleague Fred Daigle, also a Past President of the Society, spoke before you in May 1976 covering the historical evolution of secrecy practices. As he noted, the practices long preceded the formation of the United States; indeed they are conceptually inherent in society. Attorney General Levi discussed some of these concepts in a 1974 presentation before the Bar Association of the City of New York. Even the proceedings of the Congress did not become public until some fifty years after our nation was created. It is to be noted, in that connection that the press survived this initial deprivation. I shall hope to offer

- some views on the status of security classification in defense matters
- a few remarks on the merits and status of the current Executive Order 11652 and its implementation
- some comments on S-1, the Senate Bill to codify the United States Criminal Code as found in Title 18 (of the United States Code), and
- some thoughts on a legislative basis for the security classification system.

I do not plan to attempt to cover matters relating to the Department of State or the much-discussed "Executive Privilege" of witholding information – basically from the Congress. These are not unrelated questions – especially the former. But I feel discussions of executive privilege have tended to muddy the waters significantly, and discussion of foreign affairs would best be left to another time.

Despite the extensive furor over secrecy, it should be remembered that the relative amount of it is very small in comparison with the vast body of information on government functions that is regularly available; only some five percent of the information total is classified. The major fraction of that total is ascribed to the Department of Defense – not surprisingly – and it is that portion that I will be discussing.

Current Status of Classification

When considering information to present today, it occurred to me that it might be useful to understanding if we were to examine the reasons set forth in directives that are to guide in reaching a determination to classify. As Mr. Daigle noted, the current classification system is found in Executive Order 11652, and further detailed requirements are found in the National Security Council Memorandum of 17 May 1972, which became effective with the order (1 June 1972). There are, of course, additional directives that issued from the various departments and agencies. The one to which I shall refer is that of the Department of Defense – *The Information Security Program Regulation,* DoD 5200.1R. In it one finds the program to implement the executive order. Among its provisions are criteria establishing guidance on reaching a determination to classify. The main ones of these may be summarized as the information

- **provides a directly related scientific, engineering operational (tactical or strategic), or intelligence advantage**
- **would weaken the U. S. position in political or military negotiations**
- **would make us vulnerable to attack; limit or reduce the effectiveness of our forces; reduce our ability to defend ourselves successfully**
- **would reveal a capability of the U. S., not known to other nations, to obtain information or material**
- **would reveal our war plans/posture/potential, or provide a base to develop effective countermeasures to our systems.**

As one thinks about these criteria, likely few would find fault with them conceptually. If they form the basis for determination and are used correctly, why then is there "so bad a press?" Certainly the situation in 1976 is significantly different from that described by Benedict Zobrist when writing in the *Iowa Law Review* in 1973. Of the Truman Executive Order 10290 he said " . . . because of the vagueness and generality of many sections, the order was subjected to widespread criticism. The order retained the four-tiered classification system without providing much assistance in defining the variations among the classification . . . " and of 10501 from the Eisenhower period he noted, when referring to the description of the three classifications prescribed " . . . although all three categories are broad in their scope and language, the confidential definition truly opened a Pandora's Box . . . "

Remember, however, that the criteria set forth above are not contained in either the current executive order or its implementing National Security Council Directive, nor, of course, in any earlier orders – they are contained only in the Department of Defense implementation. It is worthy of mention that Mr. Zobrist did conclude that after a year plus of operations under EO 11652 that notable improvements had been made. Were he writing today four years after the order came into effect he might be even faintly enthusiastic. However, there are problems in attempting to get the sizeable amount of information necessary to operate within the Department of Defense – and its contractors – properly classified.

In the concept of guidance as presented, there necessarily is a vast amount of translating that must be done when determining a given case. Consider, in this context, an assessment made by Dr. Malcolm Currie, the Director of Defense Research and Engineering, in his unclassified presentation for fiscal year 1977 as displayed in Table 1.

TABLE 1

Technology Status – 1976

US LEADS	USSR LEADS
Integrated Circuits	High Pressure Physics
Computers	Welding
High Bypass Ratio Turbofans	Titanium Fabrication
Air-to-Air Missiles	HF Radio Propogation
Numerically Controlled Machine Tools	Magneto-Hydrodynamic Power Generation
Avionics	Anti-Ship Missiles Deployed
Composite Materials	Chemical Warfare
Inertial Instrumentation	Artillery
Precision Guided Weapons	
Satellite-Born Sensors	

EQUAL OR UNCERTAIN

High Energy Lasers
Aerodynamics
High-Yield Nuclear Weapons

This list tells us at least two things – the one is the assessment itself. The other is that determining at which point classification should be applied in the creation and manufacture of weaponry in these categories – in order to protect an advantage of the United States or not reveal a specific vulnerability on which the USSR could capitalize – is not an easy matter. It also suggests that the casual reporter would not be in a position to be certain whether a piece of information that he didn't really understand would or would not damage the United States. It goes without saying that this is likely to be true of most of us and our congressmen and women as well.

These preliminary notes lead me not too illogically to discussing the status of classification – because it is *there that many difficulties exist and problems remain to be solved.* It is perfectly true that examples of "bad" classification can be found. In our work in CNA, it's reasonable to say that I see some every day. It might be helpful also to identify an inherent problem in the system. That is that the system necessarily is hierarchical. At the apex is the President and at the first tier one has the departments – in my remarks that person is the Secretary of Defense, advised and assisted by the Joint Chiefs of Staff and its Chairman, as well as his principal subordinates. The next tier would include the secretaries of the military departments and the respective military chiefs of service. The reason why this hierarchy is important will be evident when one considers some of the language of EO 11652 and its implementing directive issued by the National Security Council. Consider the words below from the Executive Order and its implementing Directive.

> (A) *CLASSIFICATION RESPONSIBILITIES.* **A holder of classified information or material shall observe and respect the classification assigned by the originator (Section 4, EO 11652)**

and then from the NSC implementing directive:

> (B) *OBSERVANCE OF CLASSIFICATION.* **Whenever information or material classified by an official designated under "A" above is incorporated in another document or other material. . . the previously assigned security classification category shall be reflected thereon (Section 1, NSC Directive of 17 May 72)**

the point to be considered is that if one gets "bad" classification from the top one has a severe problem. It *isn't always easy to argue with the President, nor,* for that matter, the Secretary of Defense. The National Classification Management Society has espoused the classification guide as the only way to go.

As some of you may know, Executive Order 11652 is in the process of being modified. The four years of experience under it coupled with the effects of the Freedom of Information Act Amendments of 1974 – effective in 1975 – *caused a look at what things should be* changed to improve the operation.

As Mr. Daigle mentioned to you, the NCMS had taken a position in 1974 that there should be a legislative basis for the classification system - - a point to which I shall return. But, in the meantime we have made our views known concerning changes to the Executive Order.

In our view, there is no substitute for adequate guidance. What is termed the "derivative" classification problem is a real one, as you noted from the sections of the current order and its implementing directive. A person down on the totem pole would have difficulty in changing the classification of a paper from higher authority that he or she suspicioned – or even knew categorically – was overclassified. That person might have to cite such information in other documents because of a need for authority to pursue a given program, for example. It is quite possible – indeed, I have seen many instances – that the improperly classified information from a senior level is the only reason why a resulting product was classified. Consequently when we learned that changes to the order were proposed, we took the opportunity to make recommendations – concentrating on Section 4 of the order. Our recommendations relating to that particular area may assist in understanding the problem and are presented below.

> Sec. 4. *Classification.* Each person possessing classifying authority shall be held accountable for the propriety of the classifications attributed to him. Both unnecessary classification and over-classification shall be avoided. To this end, original classification authorities shall cause to be issued appropriate security classification guides in the respective subjects matter of their jurisdiction. Such guides will be created at the earliest practicable point in time but in no event later than the initial proposal for funding of a formal classified program or project. Military operational matters, intelligence matters, and similar categories also will be covered by classification guides. Further, such guides shall be examined in detail and reissued at least each second year, or earlier as changes so warrant. Insofar as practicable, guides will be unclassified and made widely available. In the case of classified supplements, these will be widely available to government and industry engaged in creating information or material requiring protection. Classification shall be solely on the basis of national security considerations. In no case

> shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security. The following rules shall apply to classification of information under this order.

The essential point is that with authoritative guidance in hand, one does not have to quarrel with the President or the Secretary of Defense or anyone to classify properly an excerpt needed in an auxiliary program report or analysis.

NCMS made other recommendations for change in Section 4 that we believe would, if incorporated, improve further the operation under the order and reduce further the overclassification problem. The entire recommendation is contained in Issue No. 2 of Vol. X of the *CM Bulletin*, March-April 1976. As of 19 July, the "For Comment" draft of the order had not been received in the respective departments. Exactly what will be found will have to await its arrival.

Relating to Legislation

It may seem that I have not addressed the principal question of legislation – and that's quite true. So I shall turn to it. It is evident, however, that what I *have* been covering is related to whether legislation would have a chance. It is undeniable that poor classification has caused many congressmen and women considerable pause when contemplating penalties for violations of secrecy as found in S-1 for example. Needless to say the press has been very vocal on much the same basis. Jack Landau speaking in 1975 for the Reporter's Committee for Freedom of the Press, in testimony before the Senate Committee holding hearings on S-1 covered a number of the points. He drew attention to the "theft" aspects then included and noted "it should be clear that the receipt of government information and its publication by the news media in the public interest is constitutionally immune under the First Amendment and can not be subject to the blanket threat of criminal prosecution merely because the government does not want the public to know what the report contains." He noted further that this approach was being found in states these days referring to New Hampshire and California. In the case of California he referred to the conviction of the Editor, Arthur Glick Kunkin and the Reporter, Gerald R. Applebaum, of *The Los Angeles Free Press* for having received and published a photographic copy of a list of state civil service employees acting as undercover narcotics agents. He observed that while the conviction was later overturned by the California Supreme Court on technical evidence grounds, it did not overturn the reasoning behind conviction of a newspaper for receiving stolen property. Referring to the existing espionage statutes, he noted that they

> " . . . both specifically in the statute and by court interpretation have been aimed at conventional saboteurs . . . " Then further he observes as unwarranted, "thus, a news reporter may be prosecuted for publishing 'national defense information' if he reasonably knows that the information 'may be used to the prejudice' of the United States' or to the advantage of a foreign power.' "

If I may observe, that is an aim for which, I believe, no apologies are required! It is specious to suggest that there is a substantial difference in outcome if information is published in a newspaper rather than surreptitously given directly to a foreign power. The instantaneous means available these days for world-wide news dissemination effectively eliminates any possible recall. And, current law does not cover the prosecution of any person who is not a government employee unless in the language of espionage. Mr. Robert L. Keuch of the Criminal Division of the Department of Justice speaking of these difficulties before the Ninth Seminar of our Society observed

> " . . . there are a vast number of people under our industrial security program . . . who have access to some of our most secure and most sensitive information for the purposes of designing weapons systems . . . so . . . a defense contractor could take the plans of our newest weapons system and attempt to give them to a national of a foreign country; he could be arrested in the act, and there would be no prosecution unless we were willing to declassify and present in court the plans for our newest weapons system . . . everyone says that Section 1125 of the proposed code which says that a foreign agent should not obtain or collect classified information is proper, and that we shouldn't have to disclose at that trial the very information we are seeking to protect.* But then they turn around and say you shouldn't be allowed to prosecute an individual in a position of trust over that classified information without disclosing the very information you are seeking to protect."

On the other hand, Senators Muskie and Bayh, among others, have expressed concern over the application of the provisions. Senator Bayh has suggested that an additional requirement be included in the law, borrowing from the Supreme Court's language in the Pentagon Papers case "that the information's disclosure must pose a 'direct, immediate, and irreparable harm to the security of the United States.' " In this context, I might comment that interpretation of these words in a given situation well would be difficult indeed. For example, it is not at all certain that providing information that would permit an adversary to develop a countermeasure to a complex weapon system could meet the test of immediacy – considering normal times to develop a countermeasure; nor would it necessarily be irreparable – in a usual connotation of the word – since, in due course, the United States could develop a different system, or modify the one compromised. However, it might cost another billion or so dollars – perhaps *that* would qualify as "a direct harm."

Even in defense of the provisions of S-1, Senator

*Author's Note: Despite the sometimes short-sighted view, an obtaining of information by one potential adversary does not equate with its being shared with others. For example, it is unreasonable to suppose that the USSR shares the fruits of its collection efforts with the Peoples Republic of China, nor for that matter, with nations of the Warsaw Pact.

Hruska, the ranking Republican member of the responsible subcommittee, remarked in 1975

> " . . . one particular area of controversy needs special mention. That is the area of punishing those who 'leak' secret government information. Let me hasten to assure the press and others, that this is still an open area to change in the Bill. We are still attempting to define that area where disclosure of government information may be made permissibly without undue harm to the nation – indeed, perhaps with benefit to the nation – and to differentiate that area from the area where disclosure would be unduly injurious in terms of national defense. I am sure all will recognize what a difficult endeavor this is . . . "

So, what is the status today? Little question that S-1 remains in limbo and will not reach a vote in the 93rd Congress. There is a comparative summary of two versions contained in the second issue of Volume X of our Society *Bulletin*. However, as I'm sure you have, the total text should be examined with its amendments. Such additional modifications as are under consideration at this time have not been put into print and perhaps will not, prior to the 94th Congress. I invite your attention also to the November 1975 issue of the *Congressional Digest*, which issue was entitled "The Question of Stronger Federal Laws to Safeguard Classified Information – Pros & Cons." As a personal observation, a point missed is the word to protect whatever advantage we may still have - - if there is any.

In a manner of speaking, the penalty legislation as contained in S-1, that we have been covering, is a bit cart-before-horseish, and I have so remarked to respective committee staff members. It appears that to some protection of information on behalf of the security of the United States can unarguably be established as an inherent power of the executive either incident to his responsibilities in the field of foreign relations or his established position of Commander-In-Chief of the Armed Forces. However, it is reasonable to conclude that prosecution of a violation of an inherent power is nothing less than tricky. Furthermore, and as pointed out by Mr. Daigle earlier, the executive is the executive is the executive. It is *not* the legislature nor the judiciary. While it's perfectly true that no law can abridge the speech and debate clause of the Constitution as it applies to legislators (and their staffs) in the performance of their functions, the mere existance of a law describing categories of information to be protected might act as a deterrent to thoughtless disclosures; the import of which could not be understood by the legislator.

Before turning to this aspect more completely, I would like to share with you what I perceive to be evolving procedural, protective steps in finding language in different but related contexts. As I mentioned at the beginning, part of the reticence to enact law has been the sometimes (too often, unfortunately) ludicrous examples of classification. A humorous historic one, of which I learned recently, pertained to the complaint in the early 1900s of the Chief of Artillery to the Adjutant General of the Army that the word "confidential" was being used indiscriminately. He pointed out the ridiculous situation of an issuance for whitewash formula being so stamped, and recommended that a time limit be set. I suppose that there well could be today those who would consider the formula for an effective whitewash to be of great significance – considering the many controversies in which it is alleged to be used.

However, in the most recent formal amendment to S-1, for example, a prosecution would be barred under Section 1124 unless under law or executive order there were (the words are *my* adaptation)

- an agency responsible (the Interagency Classification Review Committee, for example) for insuring that everybody toes the mark on classification
- a review procedure available to a person charged to consider and determine the propriety and lawfulness of the classification of the information in controversy, and
- a joint determination by the head of the Classifying Agency, the Monitoring Agency, and the Attorney General (within the past year) that the information in contention was lawfully subject to classification at the time of the offense.

Eventually these words are found also in the recommendation of the President in February of this year, for amendment to the National Security Act of 1947 relating to the protection of intelligence sources and methods. The language has been evolving since earlier versions of S-1 and it seems reasonable to note that if there is to be a prosecution, there should be at least this kind of treatment to protect whomever against caprice – for revealing a 1900-vintage whitewash formula, for example. But when such remedies exist (in *a priori* time) the necessary complement is that the law need provide that disclosure of the information be not required, in order to obtain conviction.

A current case in point. Some of you may be aware of the case of Sahag Dedeyan. In the current instance he is being prosecuted under the provisions of 18 USC 793 (f) (2). It is unusual because few (none are identified) prosecutions under this particular provision exist. Basically, the provision establishes an offense if an individual fails to report the abstracting, loss, *etc.*, of information relating to the national defense. In this case, Mr. Dedeyan, as a mathematician of capability, was employed by the Applied Physics Laboratory of the Johns Hopkins University – he was a naturalized citizen. He had a diamond-cutter cousin named Sarkis Paskalian. Dedeyan was working at home – in violation of industrial security requirements under which he and the Applied Physics Laboratory were working – when his cousin, during a visit, photographed an essentially finished document entitled *Vulnerability Analysis: U. S. Reinforcement of Nato*. His cousin Paskalian was promptly convicted as a spy when nabbed turning the film over to the Russians; He had pleaded guilty. Incidentally, some may remember that he has been proposed for spy-exchange for one of ours – unnamed – that the Russians caught. There seems little doubt about the facts. Mr. Dedeyan later was given money for his "assistance" and then and there – if not before – must have become aware of the compromise but failed to report it. The case went to trial after much preliminary activity, on July 19th. However, the judge has ruled that evidence of the propriety of classification could be presented in order to es-

tablish merit of whether a need to report existed (my words, not his). Further, and essentially without its having been noticed immediately by the Attorney General's Office, he ruled that if any portions of the document in question were to be used as evidence, the whole document would have to become part of the record. It goes without saying that in any document or report covering a major topic, much of it will be unclassified. The whole purpose of the emphasis on paragraph and section classification of the DoD Regulation to which I referred earlier, is to isolate and identify only those portions of information which themselves reveal that which should be protected. By anybody's definition, the title alone would suggest that the topic is an aspect of the war plans of the United States and the potential of NATO to exist. The mere fact that it also contains information that is unclassified is not a *prima facie* case of bad classification. We will have to see how the trial progresses but it is an unusual one that bears watching. It serves to point again, however, to the absence of legislation covering such an instance in the substance of difficulties posed to "we the people."

Concluding Observations

As Mr. Daigle presented to you in May, the NCMS is on record as favoring the establishment of a legislative basis for classification. It is not, however, in favor of the Congress managing the system. There are undeniable difficulties in establishing such a base. A few of them are:

- Definitions
- Separation of Powers
- Congressional Prerogatives
- Stifling of Appropriate Opposition

Despite some of the difficulties – none of them really small – we are living in an hostile environment and it is one of increasing complexity. It was interesting to note that Mr. Gerald L. Warren, Editor of the *San Diego Union* speaking before NCMS 12th Seminar (July 1976), observed that the press needs remember that its members too are citizens, and that there must be a balancing among its responsibilities. We good guys commonly do not fully appreciate, sometimes, the deviousness of some of our adversaries. The term "Deep Cover"* is not among those with which most of the population is familiar - - but it surely is to the USSR.

Regarding the legislative basis for the classification system, only two committees of the Congress are working in the area. One is Senator Muskie's Sobcommittee on Intergovernmental Relations of the Committee on Government Operations, and the other is Representative Abzug's Subcommittee on Government Information and Individual Rights. Neither of these has a current bill before either house. The potential approaches differ. Because Representative Abzug's subcommittee is responsible for the Freedom of Information Act, proposals have taken the form of amendment to the Act. It is not at all clear that the Freedom of Information Act is either the best or a proper place for such legislation. Senator Muskie's approach seems to trend in the direction of creating a whole cloth and seems better to me as an approach; the foundation should not be placed over an existing trellis.

It is possible, but not likely - - considering that this is an election year - - that new hearings or new bills will be introduced in this Congress. My recent discussions with committee staff do not suggest that action will be forthcoming that soon.

In these few minutes I have attempted to share with you some information and views bearing, I hope, on your study. You have set before yourselves a most difficult but pressing question. Your thoughts and recommendations surely will be welcomed by the Congress as well as by all who are involved in this complex field.

*The term "Deep Cover" may be ascribed to the counter-intelligence field as describing an agent placed in a given country whose efforts will be required only after a long period of establishing a "good guy" image in a legitimate field of endeavor.

Notes

The notes are presented in the sequence of comment in the text.

Levi, Edward H., Address before the Association of the Bar of the City of New York, 28 April 1975, on the topic of Confidentiality and Democratic Government.

Zobrist, Benedict Karl II, *Iowa Law Review,* "Reform in the Classification and Declassification of National Security Information: Nixon Executive Order 11652," Vol. 59, No. 1, October 1973.

Currie, Dr. Malcolm R., Director of Defense Research & Engineering, *The Department of Defense Program of Research, Development, Test & Evaluation, FY 1977,* Statement to the 94th Congress 2d Session, 3 February 1976, pp.II-21,22.

Landau. Jack C., as quoted in *The Congressional Digest,* Vol. 54, No. 11, November 1975, pp. 277-287.

Keuch, Robert L., *Classification Management*, Journal of the National Classification Management Society, Vol. XI, 1975, p. 10.

Bayh, Hon. Birch, *The Congressional Record*, Vol. 121, No. 132, 10 September 1975, p.SI5707.

Hruska, Hon. Roman L., *The Congressional Record*, Vol. 121, No. 104, 27 June 1975, p. S11827.

Warren, Gerald L., Editor, *San Diego Union*, in presentation contained in *Classification Management*, Journal of the National Classification Management Society, Vol. XII, No. 2, 1977, p. 6.

Ed. Note – The following is the report to which the two previous papers relate. It is in its final form but has not reached the stage of having been voted on by the membership of the Commonwealth Club. It has been provided for inclusion in our Journal because of the obvious interest it would have to our Society. The results of the voting will be made known to the Society when they are learned.

SECTION ON NATIONAL DEFENSE
Commonwealth Club of California
681 Market Street, San Francisco, CA
September 27, 1977

WHO SHOULD CONTROL SECRECY IN REGARD TO NATIONAL DEFENSE AND TO WHAT EXTENT? [1]

Final Report

I. Introduction and Background

This study topic was first proposed in 1969 at the peak of the Vietnam war. Interest continued through 1974, then in 1975-76 the topic developed greater intensity because of the 94th Congress' consideration of a proposed rewrite of Title 18, U. S. Code, better known as Senate Bill No. 1, and referred to as SB-1.[2] Interest in SB-1 was aroused by two organizations with nationwide publicity and testimony before Congress, notably The National Classification Management Society and The Freedom of Information Center, School of Journalism, University of Missouri. The (1975-76) Congressional investigations into the activities of U. S. intelligence agencies involving ten elements of the Executive Branch also added impetus to the question.[3]

Congressional investigations came at the end of a three year period, 1973-75, during which other events, without precedent in U. S. political life, involving both the 93rd and 94th Congresses, took place.[4] They included the Senate Select (Watergate) Committee's investigation of the activities of the Republican campaign committees before, during, and after the 1972 Presidential election; the investigation of and resignation of a Vice President; the Watergate Special Grand Jury's return of indictments against Watergate principals; and the House of Representatives initiation of impeachment proceedings against a President, and the televising of these proceedings. Additionally, of the three Vice Presidents of the U.S. from 10 October 1973 to 19 December 1974, two were selected by the President with the approval of Congress. One had succeeded to the Presidency. For the very first time, both an incumbent President and Vice President had been approved by Congress but not elected.

A story by reporter Seymour Hersh that appeared in the *New York Times* in 1974 quoted sources charging that "The CIA, directly violating its charter, conducted a massive, illegal domestic intelligence operation during the Nixon administration against the anti-war movement and other dissident groups in the United States."[5] Two other columnists claimed the climate surrounding these events was an attempt by some to perpetuate the Watergate climate.[6] CIA Director William Colby denied the *Times* allegations during testimony before a House Sub-Committee on February 24, 1975, granting meanwhile, that some minor stretching of the CIA charter may have occurred. Colby insisting that the actions were not massive, illegal, or domestic as charged, stated that all operations resulted from a presidential directive or stemmed from the authority of the National Security Act.[7]

In the course of these events from 1973-75, the executive branch under two different presidents was unable to protect some of its most significant national defense secrets. Defense information was broadcast throughout the world after disclosures by the Legislative and Executive Branches. The CIA Director pointed out that "We are developing a reputation in other intelligence services of not being able to keep secrets in this country."[8] Thus, the control of national defense secrets appeared irrational, and the question, "Who should control secrecy in the national defense and to what extent?", became vitally significant.

II. Media Disclosure of National Defense Information.

The media freedom to reveal any defense information they choose represents a matter of primary importance. Some media leaders have expressed the opinion that secrecy remains judgmental, with no clear-cut right or wrong answers on the subject each case resting upon its own merits.[9] For example, Daniel Schorr, the former CBS reporter who admitted taking and giving the House (Pike) Select Committee Intelligence Report to a publisher, has said that the U. S. government resides upon tension between the three branches of government, all equal, with nobody in charge; that a reporter's job is to get all government secrets he can, while the government attempts to keep all its secrets it can. The end result, according to Schorr, is that some secrets would be kept and some would not. Further, he has maintained that no one is in charge of releasing information to the public, and no one should have that responsibility.

Supreme Court Justice Potter Stewart, seemingly supporting this view, has contended that it has been only in the last two years, culminating in the resignation of President Nixon, that the public has fully realized "the enormous power that an investigative and adversary press can exert . . . ," adding that "the established American press in the past ten years, and particularly in the past two years, has performed precisely the function it was intended to perform by those who wrote the First Amendment to our Constitution." In reference to the 1971 Supreme Court refusal to restrain the *New York Times,* and others, from publishing the Pentagon Papers, he ruled, "The Pentagon Papers case involved the line between secrecy and openess in the affairs of government. The question, or at least one primary question, was whether or not that line is drawn by the Constitution itself. The Justice Department asked the Court to find

[1] *Footnotes follow the text.*

in the Constitution a basis for prohibiting the publication of allegedly stolen government documents. The Court could find no such prohibition. So fas as the Constitution goes, the autonomous press may publish what it knows, and may seek to learn what it can."[10]

On the other hand, Justice John Harlan disagreed and significantly, Chief Justice Warren Burger and Justice Harry Blackmun sided with Justice Harlan's dissent. Justice Harlan noted the new Constitutional arrangement created by the Court's decision in this case, and that the Executive Branch's determination of what should be considered "secret" deserved preference over the media's determination, explaining, "even if there is some room for the Judiciary to override the Executive determination, it is plain that the scope of the review must be exceedingly narrow. I can see no indication in the opinion of either the District Court or the Court of Appeals in the *Post* litigation that the conclusions of the Executive were given even the deference owing to an administrative agency, much less that owing to a co-equal branch of government operating within the field of its Constitutional prerogative."[11]

In its analysis of the First Amendment, the Section on National Defense has noted that the word "guarantee" does not appear in that part of the Constitution. Rather it represents a prohibition or restraint on Congress.[12] The judicial interpretation of the First Amendment is relatively recent. The late Yale Law professor Alexander Bickel stated, "The total career, robust or otherwise, of the First Amendment as part of the law of the Constitution encompasses little more than half a century. Of course, the First Amendment has been in the Constitution and has had pride of place in the Bill of Rights since 1791, so what we may think of as its admonitory career is quite long. But, its legal career in court decisions is a matter, essentially, of the past half century."

Writing about the media and the First Amendment Kevin Phillips has called attention to the recent flurry of propoganda about the public's "right to know" coupled with the media invocation of a First Amendment "free press" spirit going back to the Founding Fathers.[13] It is difficult to invoke the views of Thomas Jefferson or James Madison on behalf of the new legal rights claimed by the knowledge industry, he believes, because judicial interpretation of the First Amendment took place only in the last half century. He claimed that today's media power would have been absolutely unrecognizable by the architects of the Constitution, and the situation has deteriorated. Like past emerging economic concentrations, he continued, the communications industry is busily trying to expand a segment of the Bill of Rights (the First Amendment) to fight off regulation. To some scholars, the news media have become "the last stronghold of laissez-faire", and justly so. In other words, national security, virtually defenseless, faces danger in an unprecedented situation that finds an increasingly dominant economic interest group, i.e., the media, formulating its own rules.

III. Divided Government and Violations of Security

Does divided government -- one party in control of the Congress and another in control of the Executive Branch -- tend to cause violations of security regulation? One source has suggested that current aspects concerning secrecy in national defense are symptoms of a much larger, underlying problem, i.e., divided government with Congress of one party, the Executive of another.[14] Indeed, divided government has existed in 14 of the last 24 years, or almost 60% of the time, creating an unprecedented situation. During the preceding 164 years under the Constitution, divided government took place only 8% of the time.[15] During the period (1969-1976) in which divided government has existed, an attempted impeachment of a President occurred, the second such event in U. S. history. (The first also came during a divided government at the time of the 40th Congress, 1967-1969.) The 93rd and 94th Congresses have conducted investigations, hearings, and the release of classified information in a manner and to a degree unprecedented. Party discipline therefore, seems to be the key to having Congress respect secrecy in national defense. A Congress of the President's party rarely, if ever, breach security because of the political consequences from their own party disciplinary machinery.[16] Legislation, experts argue, is not the answer. Congress will not divest itself of such a political weapon, and it frequently declares itself exempt from legislation applicable to all others. As an example, Congress declared itself outside the provisions of the 1964 Civil Rights Act. Perhaps as some believe, security violations represent the burden of divided government.

A press account illustrates political infighting in the course of investigations:

> "By fall 1975, the traditional jealousy between the House and the Senate had flared up behind the scenes, and Mitchel Rogovin (CIA Special Counsel) negotiating with both committees, was finding them competitive. 'Church', says Rogovin, 'held his toxin hearings' because he was afraid Pike would do it if he didn't . . . By December, the House and Senate Committees were set on opposite courses. Pike wanted to impale the CIA for its abuses. Church wanted to show that a Senate committee could handle national secrets responsibly. The Ford administration played the committees against each other.
>
> "No single event did more to turn public opinion against the investigations than the assassination of Richard Welch, CIA station chief in Greece. As 1975 ended, the press was shying away from the CIA issue, and hostility toward the inquiry was building up in Congress itself."[17]

Divided government incorporates a system of checks and balances. One of the strengths of our constitutional system, is the keeping of one party from becoming too powerful. A Congress in control of a party opposite to that of the Executive restrains what historian Arthur Schlesinger of New York University calls the "Imperial Presidency."[18]

Violations of security thus inherently occur in divided government frequently necessary in order that the citizenry be protected against a government which may violate its civil rights. Individual rights transcend all but the most vital government national defense secrets. In any event, the Supreme Court has held that government secrets, even if allegedly stolen, may be published, since the Constitution, ***per se,*** does not prohibit such action.

IV. Bureaucracy

Some experts maintain that secrecy is a disease characteristic of all bureaucracies.[19] It springs spontaneously but informally at all levels, and represents a convenient method of covering mistakes. The government's present classification system, created by its bureaucracy, needs overhaul since it results in over-classification of non-sensitive materials and wastes money. As an example, a study group, after surveying Lockheed's huge stock of documents on antisubmarine warfare, recommended that 90% of the information be declassified. Large sums are expended to store and protect documents and materials which need little or no protection.

The enemy's information gathering techniques in our society are so effective, that the government's security system does little to hinder them. On the other hand, the public cannot obtain information, because of artificial bureaucratic barriers. The President, others insist, should establish national defense classification criteria. Congress, functioning only as a watch-dog should not assume constitutionally based Executive functions, although it must be kept informed.

The existence of a bureaucracy, nonetheless, does not change the nation's need to protect its national defense secrets.[20] Even though the American people may claim a "right to know," the individuals within the intelligence agencies and combat troops who represent those same American people sometimes need the cloak of secrecy; its absence increases their peril.

Secrecy, of course, remains essential for the protection of sources of information. Granting that bureaucracy constitutes the prime problem, however, it should be reduced. Sanitized information should be given to the public so that it may know the basis for high level decisions. Only critical information should be withheld.

Thus while the necessity for some secrecy is recognized, its misuse has caused government to lose credibility. Better classification criteria and frequent reviews might prevent over-classification and keep the system from being counter productive. In this regard, we note that the Office of the Secretary of Defense (OSD) does coordinate classification policies among the services and tries to facilitate an exchange of information.

V. Maintaining the Status Quo of Security Regulations

Executive Order No. 11652,[20] the basis for the current DoD Information Security Program, clearly makes *information available to the American people, provided* that the information will not harm the national interest, or that of our allies. The National Security Council implements the Order through its administrative machinery as does DoD Directive 5200.1[21] which also prohibits covering mistakes or inefficiencies in the name of national defense. The Assistant Secretary of Defense)ASD) (Comptroller) insures compliance within the DoD through his own Classification Review Board (CRB) and the Information Security Advisory Board (ISAB). Control of original classification authority, a key point, is restricted solely to those officials specifically designated in writing by DoD Reg. 5200.1R and may not be delegated. Designations of this authority are limited to the minimum. Administrative convenience alone is not a valid basis for requesting or granting this authority. Each classifier is held accountable for the propriety of his classification, whether originating his own document or interpreting source documents. The classifier is required to maintain a record showing the basis for his classification or a system by which a chain of classification authority can be traced. He must take into consideration the degree of intended dissemination, use of the material, and whether the end purpose nullifies effective security control. Each document is classified on the basis of the most sensitive information it reveals. Appearance in the public domain does not preclude initial or continued classification; however, if specific classified information is compromised, the original classifier re-evaluates the classification.

Accurate, uniform and consistent classification systems and equipment under research, development, test, or evaluation are issued. Classification in industrial operations is based on guidance furnished by the U. S. government: contractors do not make the original determinations. They apply the classification decisions of the U. S. agency for which they work. Industry must insure the number of people responsible for applying U. S. classification decisions is minimized.

Penalties exist for the compromise of classified information. Immediate action is taken to negate unauthorized disclosures. Action is also initiated to regain custody of material when appropriate and identify the compromised data. Any person who has knowledge of possible compromise of classified information must report it immediately. The penalties for gathering, transmitting, or losing defense information are addressed in Section 293 of Title 18 of the U. S. Code.[22] Some authorities believe that the President's Executive Order No. 11652, the U. S. Code and the implementation within the military departments, makes the DoD security program adequate for a democratic republic. Furthermore, tighter controls are inconsistent with U. S. Constitutional principles.

Others maintain that the current government secrecy program appears adequate but in practice has been relatively ineffective.[23] According to the U. S. Code, penalties cannot be enforced, for example, unless it can be proven that a violater "believed" his information could injure the U. S., or to have "lost" the information through "gross negligence." Enforcement, therefore, has been difficult. Statistics show accused violators have a better than even chance of avoiding conviction. Limitation of original classification authority does not preclude interpretation of classification guidelines by minor officials. Over classification and proliferation of documents continues.

Administrative action against military violators is not consistent. Efficiency reports or performance ratings containing data on security violations can be stricken from individual personnel files. Such eliminations may remove the only record of individual mishandling of sensitive material. Industry holds an estimated 70% to 80% of classified national defense data. Although the government provides for the protection and handling of this material by the Industrial Security Management Program, the primary weakness centers on the lack of criminal sanctions with which to prosecute the non-military violators for offenses short of espionage.

VI. Provisions By Congress of Legislative Base For Security Regulations

The major question thus arises: should regulations on secrecy be continued in status quo as to content, but with a legislative base provided for the regulations?

Some observers believe that the U. S. Code, Title 18, should be expanded to provide criminal sanctions for those individuals who after being entrusted with classified information, breach that trust, disclosing it to an unauthorized person.[24] In their view, the intent to harm the United States and advantage a foreign power should relate only to the severity of the sanction. The United States government expends large amounts of money each year administering programs of classifying that information considered sensitive in the interest of national security and determining who may be entrusted with national secrets. Each individual granted various positions of trust receives briefings as to proper handling and disclosure. It would appear inconsistent with the best interests of the United States if the act of releasing classified information by such a trained individual were considered less than a crime.

On the other hand, opponents of criminal sanctions point out that only harm to the United States or assistance to a foreign power makes the act effectual. This contention holds that the establishment of harm to the United States or value to a foreign power may, in most cases, would be speculative. The unauthorized disclosure may simply initiate a series of disclosures that result in unintentional harm to the United States or benefit a foreign power. If an unauthorized disclosure is criminal only when it is proven to be harmful to the United States or to be of assistance to a foreign power, significant void in the efforts to protect national security ininformation would result.[25]

Some insist that the criminalization of disclosures of classified information which does not result in harm to the United States or aid to a foreign power would be repressive for several reasons. For example, it would deter the disclosing of governmental misdeeds that were classified for the simple purpose of hiding them. Additionally, it would provide another threat to be used against those individuals who might be considered unfriendly to a current political power structure, and might very well upset the balance between the public right to know and the government's responsibility to provide for the common defense.[26]

Those who believe that the government's national security information program needs a statutory base contend that legislation should be enacted to provide a statutory base for our National Defense Information Program. The legislation should be directed at program policy rather than managing the details of the program. It should include a definition of national security, defense information, or information requiring protection in the interest of national security. This should be established by category and include recognition of international agreements relating to the interchange of classified information, e.g., NATO information, etc. It should also define classification and declassification authority, establish congressional monitoring and oversight organization, and program violations as crimes for which punishment provisions would be established.

Advocates insist that a statutory base would improve the current Executive Order by providing an unambiguous applicability to all branches of government. Furthermore, the legislation would provide a more stable existence for this very important national program. As it now stands, the President can issue or reissue an executive order at his pleasure and with consultations only to a level he considers adequate. The enactment of criminal sanctions, would establish a much needed deterrent. It is questionable that such a program should be expected to protect our national interest without incorporating effective deterrents. Advocates say that by providing the program with a statutory base, the individuals responsible for its administration would have clearcut stable objectives.

Finally, it seems only appropriate that our government's national defense information program, the success of which so greatly impacts on our national security, should be founded in legislation rather than an Executive Order. The joint wisdom of the Executive and Legislative branches should provide this vital program with greater insight.

According to the Department of Justice, no official position exists on legislation for the government's national security information program. The Department has had no opportunity to comment on such legislation for the following reasons: Such a base is totally unnecessary, it raises some very serious constitutional questions; and the Legislative Branch record in analogous attempts has not been very productive.

An inherent executive responsibility to protect classified information exists. It is the inherent power charged of the executive to protect the country from foreign attack, to provide a constitutional system, and to establish that we shall have a republic. Classification of information is a part of that power.

The question arises: Can any legislation be passed which would reduce or limit the discretion of the President (or Executive Branch) to act in defining classified information? Once an item is on the statute books, it becomes frozen. Congress is slow, even reluctant, to act in this area. As an example, the Brown Commission report, which was a codification of the Federal Criminal Code, contained in S-1 or S-1400, has lingered in Congress for over four years. When Congress acts in an area it considers extremely important to national defense, where future contingencies are unpredictable, there's a tendency to grant broad powers, such as 18 USC 793,[27] because to do otherwise would make Congress responsible for having granted the Executive insufficient authority to act in the national defense. Congress wanted to make the statute sufficiently all-inclusive to take care of changing contingencies. What may be considered unessential to national security today, may be considered essential at a later date, and vice versa.

A needed change in an administrative procedure, for example, for the Inter-Agency Classification Review Committee can be made much more quickly by an Executive Order than by going the legislative route.

Senator Alan Cranston has announced that he will oppose any effort in Congress to impose civil or criminal penalties on government employees who leak classified information to the press.[28] He believes choking off news at its source is a subtle, but effective, form of prior restraint and censorship; that the greatest deterrent to

wrongdoing or folly in government is fear of public disclosure; that we must not muzzle federal employees who in good conscience reveal violations of the law or wrong behavior; that the U. S. doesn't need more secrecy laws; that we already have strong criminal laws against espionage, theft of government property, and improper disclosure of intelligence information.

VII. Liberalization of Security Regulations

Official secrecy principles are based on both law and practice. Security classification of information is included within the President's war powers, as further delineated in the National Security Act and the Atomic Energy Act (1954). Criteria are established by Executive Order for necessary control of classified material. The Freedom of Information Act seeks release of data, but exempts matters specifically required to be kept a secret. Recognizing the "need to know" doctrine is based on both law and practice, the philosophy of secrecy seems to be based on the proposition that the fewer people who know, the greater the security, and only those who need to know should know. Defects in the "need to know" doctrine, however, are obvious. Those who already "know" decide who "needs to know." The result: secrecy can be used to hide mistakes. And, it inhibits questioning whether secrecy in a particular case serves the national interest.

The excessive volumes of secret material threatens security. James Burnham has written that "There is only one way to have an absolute guarantee against leaks, and that is to have no secrets. Cut down to one percent of its present size, the secrecy stockpile would still be large enough to include everything that really needs to be hidden from us laymen. Thus shrunk, it would be 100 times easier to protect (psychologically and politically as well as physically easier) from prying eyes and babbling mouths."[29]

Knowledge, however, is essential to a reasoned decision. For example, the First Amendment to the Constitution restrained the new government from blocking the way of information to the people via speech or press. Later, court decisions have broadened its provisions to a virtual guarantee of freedom of speech and press. The Freedom of Information Act (5 USC 552) further protects the citizen's ability to determine whether or not his government is doing a proper job. It opens Executive Branch records to him, with certain exceptions, provided he can specify the documents he seeks.

Secrecy as a danger can be illustrated by two examples of governmental assaults upon the environment through actions of governmental agencies. The first of these deals with the increased radioactivity due to nuclear bomb tests in the high atmosphere.[30] The Army concealed the killing of 6,000 sheep by stored nerve gas gas in Utah. With revelation, public pressure led to a reversal of a decision to dump the gas into the Atlantic, when it became known that safer means of disposal existed.

The use of secrecy to conceal blunders is also illustrated by a secret General Accounting Office report indicating U. S. armored forces in Europe were "woefully deficient" in readiness. The report might have given valuable information to the Warsaw Pact. Senator Humphrey revealed a summary of the report presumably to force correction.[31]

A policy of liberalization of the secrecy system would avoid introducing criminal sanctions against those who reveal classified information without proven "intent to damage the country or aid its enemies." A law making revelation of classified information a crime without the present intent provisions would add greatly to the power of the Executive Branch to keep matters secret, although it can be argued that in several recent cases it has proven better that some secrets were revealed.

It appears that the present security system provides an adequate balance between security and providing adequate information to the public. The examples given in the "pro" argument, where official secrecy delayed correction, ended with the needed information revealed and action taken to protect the values or rights of the majority. A society in which the *New York Times* could publish the Pentagon Papers, and in which a President could be driven from office over an unsuccessful attempt to cover up a politically motivated third-rate burglary, is not threatened by excessive official secrecy. Ours is one of the most open societies on earth. It may be questioned whether we can keep our secrets well enough to be trusted by our allies.

VIII. Analysis and Summary

The question "Who should control secrecy in national defense?" cannot be answered in a manner legally and politically acceptable. It can only be answered logically. The President should control secrecy in national defense, because he, under the Constitution, Article II Section 2, is Commander-in-Chief. Only he is responsible for all military operations, strategic and tactical, administrative and logistical. Only he is in position to know how all classified data affects the national defense. Under present practices, when the Legislative or Judicial Branches comes into possession of defense information classified by the Executive Branch, the protection of such classified information is at the discretion of the individual legislators or judges concerned. Recent examples of the exercise of such discretion by the Legislative and Judicial Branches include the release of classified data obtained during the CIA hearings by the former, and the decision by the latter to release the Pentagon Papers.

The Section's study tends to suggest that the President can control defense information only to the extent that the Legislative Branch and the media, together with their numerous allies and supporters both in and out of government, would permit. The Judiciary Branch occasionally determines the "extent of control", but with much less frequency than the others. In effect, elements of the government not responsible for the control of secrecy, combined with the media, exercise a greater determination over the release of classified defense information that does the responsible official and department. This was clearly pointed up by Justice Harlan in his dissent in the Pentagon Papers case. Realistically, and particularly for the immediate future, it appears that the degree to which the Executive can fulfill his responsibilities for secrecy in national defense will depend on the political approval that the media, Congress and the Judiciary Branch choose to extend to the President. It could be that this triple alliance has succeeded in establishing such precedents that a president may never have

the authority commensurate with the responsibility he carries in this field.

QUESTIONS AND ARGUMENTS

1. *Should Congress enact legislation for the classification, preservation and disclosure of national security matters?*

PRO: The classification and protection of national defense information is so important that Congress should give it a legal basis. With the exception of espionage, for which intent must be proved, and the Atomic Energy Act, there is no broad legislative base for protection of national security information. Moreover, Congress should be subject to its own statutes for the security of such information. Congress should not be permitted to use the leaking of classified national defense information as a domestic political weapon against the Executive Branch for domestic political advantage of any type.

CON: It is an inherent Executive Branch responsibility to protect classified information. If Congress legislated in this area it would have "to make a law abridging the freedom of speech or of the press." This is contrary to the First Amendment. For Congress to criminalize disclosure of classified information would tend to deter government workers from disclosing misdeeds that had been classified simply for the purpose of hiding them. Such legislation could well upset the balance between the public's right to know and the government's responsibility to provide for the common defense.

2. *Should regulations on security matters:*

a. Remain unchanged?

PRO: Between the President's Executive Order No. 11652[32], the U. S. Code Title 18[33], and the implementation within the military departments, the Department of Defense security program is adequate for a democratic republic. Tighter controls would be inconsistent with U. S. constitutional principles.

CON: The current government secrecy program appears adequate, but in practice it has been relatively ineffective. The "intent to harm the U. S." or "gross negligence" are difficult to prove. Statistics show accused violators have a better than even chance of avoiding conviction. A legislative base setting more precise criteria is needed.

b. Be liberalized?

PRO: The excessive volumes of secret material threatens security. Cut down to one per cent of its present size, the classified stockpile would still be large enough to include everything that really needs to be hidden from the layman. The public needs to have access to more, not less, information in order to reach reasoned decisions. The liberalization of security regulations is necessary to achieve this purpose.

CON: To liberalize security regulations would make the situation worse than it is now. Society is not threatened by excessive official secrecy. Ours is one of the most open societies on earth. The question has already arisen as to whether we can keep our own secrets well enough for our allies to trust us with theirs.

3. *Should the media have total freedom to publish/broadcast any information they choose?*

PRO: There is no one in charge of releasing information to the public, and no one should be. In the U. S. system everyone does what he's supposed to do and we hope it comes out right. There can be no clear cut right or wrong answers on secrecy in national defense. So far as the Constitution goes, the autonomous press may publish what it knows, and may seek to learn what it can. The media's job is to obtain all government secrets it can while the government attempts to keep all the secrets it can. Damage that may come to the latter by disclosures of the former is a price that has to be paid to keep the public informed.

CON: The Executive Branch's determination of what should be considered secret deserves preference over the media's determination. The First Amendment of the Constitution is a prohibition on Congress and not a guarantee to the press. The legal (Supreme Court) history of the First Amendment is only about 50 years old. The communications industry is busily trying to expand a segment of the Bill of Rights (First Amendment) to fight off government regulation. The media have become the last stronghold of "laissez-faire." The public interest has virtually no legal status or access.

GLOSSARY

The Assistant Secretary of Defense (Comptroller) is the senior DoD official having authority and responsibility for compliance of Executive Order 11652 and NSC directives. His Deputy for Security Policy is responsible for the development of policies, standards, criteria and procedures governing the DoD Information Security Program.

Classification – The determination that official information requires a specific degree of protection.

Classifier – An individual who determines that official information requires classification or that information of the same substance is already classified.

Compromise – Known or suspected exposure of classified information or material to an unauthorized person.

Document – Any recorded information, regardless of form.

Department of Defense Information Security Program is promulgated by DoD Directive 5200.1 dated 1 June 72. The directive warns against the use of security classification measures to conceal administrative error or inefficiency, prevent personal or departmental embarrassment, restrain competition or independent initiative, or to prevent the release of official information which does not require protection in the interest of national security.

1. Classification, when determined to be required, shall be retained for the minimum length of time commensurate with its degree of sensitivity, cost and probability of compromise.
2. When classified information requires a lower level of protection or no protection at all, it shall be regarded as declassified completely.

Department of Defense Regulation 5200.1 dated 15 Nov. 73 covers the classification, downgrading, declassifying and safeguarding information and applies to all DoD activities. While supplementary instructions or directives are unnecessary at DoD level, military departments do publish clarification and guidance. The regulations establishes the basis for identification

of information to be protected; prescribes a progressive system for classification, downgrading and declassification; prescribes safeguarding policies and procedures to be followed; and establishes a monitoring system to insure effectiveness of the Information Security Program.

DoD Classification Review Committee corresponds to the ICRC. It receives, considers, and acts on suggestions and complaints on the DoD Information Security Program. Important aspects of this responsibility include the areas of overclassification, unnecessary classification, failure to declassify or delay in declassifying.

DoD Information Security Advisory Board is composed of senior Defense Department officials. The board is advisory, reviewing DoD Security Programs and recommending new or revised uniform policies or criteria to meet changing conditions or correct program deficiencies.

Executive Order No. 11652 dated 8 March 72 is entitled "Classification and Declassification of National Security Information and Material" and is the basis of current DoD Information Security Program. It states in part: "The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public." But within the federal government there is some official information and material which, because it bears directly on the effectiveness of our national defense and conduct of our foreign relations, must be subject to some constraints for the security of our nation and the safety of our people and our allies.

Freedom of Information Center — an activity of the School of Journalism, University of Missouri at Columbia which conducts a continuing study of governmental secrecy.

National Classification Management Society (NCMS) — A non-profit organization of industrial and governmental classification managers headquartered in Alexandria, VA.

The National Security Council (NSC) monitors the implementation of Executive Order 11652. To assist the NSC in Inter-Agency Classification Review Committee (ICRC) has been established. The ICRC overseas actions of all executive departments to insure compliance with provisions of the order and implementing NSC directives. Most importantly, the ICRC seeks to:

1. Prevent overclassification;
2. Insure prompt declassification;
3. Facilitate access to declassified material;
4. Eliminate unauthorized disclosure of classified information.

Senate Bill No. 1 (SB-1) — A proposed rewrite of Title 18, U. S. Code. Section 1124 of the bill would make it a criminal offense to disclose classified information to an unauthorized person; however, it would not make receiving such information a criminal offense. The bill died at the end of the 94th Congress. Two civilian agencies in particular expressed concern over the demise of SB-1: The National Classification Management Society and Freedom of Information Center, University of Missouri.

Title 18 of the United States Code (Espionage Law) section 793 states: Whoever, for the purpose of obtaining defense information believing it is to be used to injure the U. S. or to the advantage of foreign powers, shall be fined not more than $10,000, 10 years in prison or both. Whoever receives or attempts to receive classified material shall be fined $10,000, 10 years in prison or both. Whoever willfully communicates/transmits information which the person has reason to believe could injure the U. S. will be penalized as above. Whoever through gross neglect, permits removal or loss shall also be fined the same as above.

Note: The principal investigators for this study were:
Henry J. Armstrong, RADM, USN (Ret)
Elias C. Townsend, BGEN, USA (Ret)
Anthony Johnson, LTC, USA, Hq. Sixth U.S. Army
John D. Tippit, President, WASP Enterprises, Inc.

Footnotes

1. Control, for the purpose of this report, encompasses a variety of component functions such as describing standards, regulating procedures, enforcing punitive provisions, compliance, reviewing developments and releasing materials from classification.
2. see glossary
3. Report of the Senate Select Committee on Intelligence (Church Committee), 94th Congress, 1976. From the House Select Committee on Intelligence, (Pike Committee), 94th Congress, 1976.
4. The 1976 *World Almanac,* the *New York Times* and *San Francisco Examiner* and *Chronicle.*
5. Hersh, Seymour, *New York Times,* December 22, 1974.
6. Chamberlain, John, *San Francisco Examiner,* January 20, 1975.
7. Colby, William, Director of CIA, replied to the *New York Times* accusation in the public testimony before a House Sub-Committee on February 20, 1975.
8. Colby, William, Director of CIA, *U. S. News and World Report* Interview, August 18, 1975.
9. Murphy, Reginald, Editor, *San Francisco Examiner,* address to the National Defense Section, June 10, 1976, on the subject, "Should The File Cabinets Be Locked?"
10. Schorr, Daniel, Comments during interview, Dinah Shore Show, Channel 44, Tuesday, March 15, 1977.
11. Potter, Stewart, Chief Justice, U. S. Supreme Court, in an address to Yale Law School on its 50th Anniversary, November 2, 1974, as reported in the *Wall Street Journal*, on January 13, 1975, by Ed Cony.
12. Bethel, Tom, "The Myth of An Adversary Press," *Harper's,* January 1977.
13. *First Amendment to the United States Constitution.*
14. Phillips, Kevin, "A Matter of Privilege," *Harper's,* January 1977.
15. Townsend, E. C. Maj. Gen. USA (Ret), address to the National Defense Section, July 15, 1976, on the subject "An Overall Analysis: Who Should Control Secrecy in Regard to National Defense?"
16. Historical Statistics, Dept. of Commerce, Bureau of Census, Bicentennial Edition, pgs. 1083-1084.
17. *New York Times* article appearing in the *San Fran-*

cisco Chronicle/Examiner on September 19, 1976.
18. *The Imperial Presidency,* by Schlesinger, published by Houghton-Mifflin.
19. Possony, Stefan T., Ph.D., Hoover Institution on War and Peace. Address to the National Defense Section, August 11, 1976, "A Look At Secrecy In National Defense."
20. refer to No. 19
20. see glossary
21. see glossary
22. see glossary
23. Daigle, Fred, Commander, USN (Ret). Address on May 6, 1976, on the subject "Classification Management and Secrecy.
24. refer to No. 23.
25. Keuch, Robert L., Deputy Chief Appellate Section, Criminal Division, Department of Justice. Remarks given before the National Classification Management Society.
26. Remarks given by Senators Birch Bayh and Edmond S. Muskie, in the U. S. Senate, *Congressional Digest,* November 1975, under Titles, "The Question Of Stronger Federal Laws to Safeguard Classified Information."
27. see glossary
28. Fogarty, John, "Cranston Opposes Penalty For Leaks." *San Francisco Chronicle,* March 19, 1977.
29. Burnham, James, "Secrets," *National Review,* June 20, 1975.
30. Commoner, Barry, *The Closing Circle,* Alfred A. Knopf, Inc., 1971, p.199.
31. *San Francisco Chronicle,* July 9, 1976, p. 16.
32. see glossary
33. see glossary

Ed. Note: The following is the text of the draft Executive Order prepared by the Board of Directors of the Society in a special meeting called for that purpose. It was submitted by the Society President by letter and the letter along with notes summarizing the important points was contained in *C/M Bulletin* No. 4, Vol. XI, Jul-Aug 1977. In this presentation the notes will not be repeated and the Table of Contents will be omitted. The substance of the Order and the points included or excluded are based on the views of the Society members as expressed in response to survey, at seminars, training sessions, and the like. They have a substantial background and rationale to support them.

5 August 1977

Mr. Robert Gates
National Security Council
Executive Office of the President
Washington, D.C. 20506

Dear Mr. Gates:

We have fortuitously encountered a copy of an early draft of the forthcoming Executive Order which will replace EO 11652. We believe this draft was prepared about the third week of July.

As you will remember, the Society, on earlier occasions, has made recommendations aimed towards improving the National Security Information and Material Program. Further to that end, the Board of Directors of the Society was convened to consider the draft and how it contributes to the effectiveness of the overall program. The Board represents a collection of management and operational experience in the field of information security and related matters well in excess of 200 years. This experience includes but is not limited to DoD and the Military Departments, ERDA, the intelligence community, NARS and other government agencies and industry.

We were pleased to note improvements in the requirements for the program which are in consonance with our prior recommendations, including the elimination of some unnecessary requirements within the existing system. In our considered view, however, further improvements are needed if the goal of the program is to be achieved. We have prepared modifications to the draft described which we believe will:

- Strengthen features which we strongly believe are critical for the success of the program
- Collect like functions together within the Order to facilitate understanding of the requirements of the program
- Improve the clarity of the Order and aid in the implementation of the program.

It is, perhaps, worth noting that this program is not a simple matter. However, we believe that management of the program may be further simplified and still meet the requirements set forth by the President. We do recognize that, given the requirements of the program, a high-level of knowledge and competence is essential to reach supportable conclusions relating to the need to protect official information in the interests of national security.

We submit the results of our study for your consideration. They are presented in the form of a revised draft; one copy being presented with rationale following the related section, and one with rationale presented separately. It is our firm conviction that the recommendations we make would result in important improvements in the program and that they are feasible.

We express our appreciation for the opportunity to present our views. You will recognize, I am sure, that in the press of time we have not been able to develop as complete and finished a presentation as we would desire and the subject warrants.

We would be pleased to offer such additional comments as you would find helpful for the Order or its implementing directive.

Most sincerely,

James A. Buckland
President

TITLE 3 – THE PRESIDENT

Executive Order 1---- **September , 1977**

National Security Information and Material

To ensure that national security information shall be protected, but only to the extent and for such period as is necessary, and bearing in mind the need to provide for the fullest possible flow of information to the public, this Order identifies the information to be protected, prescribes procedures for classifying, declassifying, downgrading, and safeguarding that information, and establishes a monitoring system;

Now Therefore, by virtue of the authority vested in me by the Constitution of the United States it is hereby ordered:

SECTION 1. Classification of Information.

Offician information or material which requires

protection in the interest of national security against unauthorized disclosure shall be classified at one of the three levels Top Secret, Secret, or Confidential, as defined in Section 2; dependent on the degree of its significance to the national security.

SECTION 2. Definitions

Confidential That information or material the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

Department As used herein, includes Agency or other governmental entity.

Intelligence The product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas, which is immediately or potentially significant to the development and execution of plans, policies, and operations.

National Security Information That information which is essential to the national defense or foreign relations of the United States.

Official Information That information which is owned by, produced for or by, or is subject to the control of the United States Government.

Secret That information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

Sensitive Intelligence Methods The means by which support is provided to sensitive intelligence sources or the means by which intelligence is received from sensitive intelligence sources, when such means are vulnerable to counteraction or to loss of essential privacy if they are compromised.

Sensitive Intelligence Sources A person, organization, or technical means which provides intelligence, and which is vulnerable to counteraction and thus could be lost or diminished in effectiveness if its identity is compromised. A sensitive Intelligence source is also a person or organization which provides intelligence subject to agreement to protect its identity and intelligence relationship.

Top Secret That information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

SECTION 3. Original Classification

(a) *Classification Criteria.* Information may be classified under this Order only when it is official information, when it meets one of more of the following criteria, *and* when its unauthorized disclosure could reasonably be expected to cause damage to the national security. The criteria apply equally to the three levels of classification defined in this Order.

(1) The information is reasonably expected to provide the United States, in comparison with other nations, with a scientific, engineering, technical, operational, intelligence, strategic or tactical advantage directly related to the national security.

(2) Disclosure of the information would reasonably be expected to weaken the position of the United States in the discussion, avoidance, or peaceful resolution of potential or existing international differences which, if not avoided or resolved, could generate a threat to the United States or its mutual security arrangements, create or increase international tensions adverse to the national security of the United States, impair foreign relations, or lead to hostile political, economic, or military action against the United States or its allies.

(3) Disclosure of the information would weaken the ability of the United States to wage war or defend itself, limit the effectiveness of its armed forces, or make the United States vulnerable to attack.

(4) Disclosure of the information would alert other nations or non-national entities that the United States has, or is capable of obtaining, certain foreign information or material of importance to the national security.

(5) Disclosure of the information would jeopardize cryptology devices and systems, intelligence sources or intelligence methods, or defense, diplomatic or intelligence operations which are essential to the ability of the United States to defend itself against a hostile action or threat or to conduct foreign relations.

(6) There is reason to believe that disclosure of the information would, to an extent not otherwise possible:

A. Provide a foreign nation with an insight into the war potential or the war or defense plans or posture of the United States;

B. Aid a foreign nation to develop, improve or refine a similar item of war potential;

C. Provide a foreign national with a base upon which to develop effective countermeasures agains United States plans or capabilities;

D. Weaken or nullify the effectiveness of a defense, military or intelligence plan, operation, project or activity which is essential to the national security.

(7) The information is required by statute to be classified.

(8) The information was provided by a foreign government, international organization, or non-national entity and *(i)*, the information is marked with a classification assigned by the source, or *(ii)*, the information would logically be assigned a U.S. classification since it meets the damage criteria for national security as defined in this Order.

(b) *Prohibitions* Classification of official information is subject to the following prohibitions:

(1) In no case shall information be classified in order to prevent or delay the release of information that does not require protection in the interest of national security. In particular, information shall not be classified in order to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person or Department, or to restrain competition or independent initiative.

(2) Basic scientific research and results thereof, except that which is directly related to the national security and meets the criteria for classification established herein, shall not be classified.

(3) Until and unless the government acquires an official interest in the information, a product of independent research and development which does not incorporate or reveal classified information to which the producer or developer was given prior access, shall not be classified.

(4) Reference to a classified document shall not be classified when that reference standing alone or in context does not reveal classified information.

(5) In any instance where classified information is released by an authorized official of the Executive Branch in an official statement determined to be publicly releasable, that information is automatically declassified. Inadvertent and unauthorized releases will be subject to determination of whether protection can or should be continued.

(6) Classification shall not be used for the sole purpose of limiting dissemination of information.

(7) Unnecessary classification chall be scrupulously avoided.

(c) *Resolution of Doubt*. If the classifier has any substantial doubt as to which security classification level is appropriate, or whether the information or material should be classified at all, the classifier should designate the less restrictive treatment.

SECTION 4. Authority to Classify and Accountability

The authority to originate the classification of official information or material under this Order shall be restricted to officials whose duties and responsibilities require the exercise of original classification on a regular and recurring basis.

(a) *Top Secret.* The authority to originate the classification of official information or material under this Order as Top Secret shall be exercised only by such officials as the President may designate in writing and by the heads of the Departments listed below and such of their principal subordinate officials as the heads of such Departments designate in writing:

Department of State
Department of Defense
Department of the Army
Department of the Navy
Department of the Air Force
Department of Justice
Department of Treasury
Central Intelligence Agency
Director of Central Intelligence
Arms Control and Disarmament Agency
Energy Research and Development Administration/
Department of Energy
General Services Administration
(Delegable only to Federal Preparedness Agency)

(b) *Secret*. The authority to originally classify information or material under this Order as Secret shall be exercised only by:

(1) Officials who have Top Secret classification authority

(2) Such subordinates as officials with Top Secret classification authority under (a) above designate in writing; and,

(3) The heads of the following named Departments and such of their principal subordinate officials as the heads of such Departments designate in writing:

Department of Commerce
Department of Transportation
Agency for International Development
Office of Micronesian Status Negotiations
United States Information Agency

(c) *Confidential*. The authority to originally classify information or material under this Order as Confidential shall be exercised only by

(1) Officials who have Top Secret or Secret classification authority

(2) Such subordinates as officials with Top Secret or Secret classification authority under (a) or (b) above designate in writing; and,

(3) The heads of the following named Departments and such of their principal subordinate officials as the heads of such Departments designate in writing

Department of Labor
Export-Import Bank of the United States
Overseas Private Investment Corporation

(d) *Designation Procedures*. The authority to originally classify information or material under this Order shall be granted to an official by name or by title of the position held by him or her. The exercise of such authority shall be restricted to such designated officials, and in their absence, to those officials specifically designated to act for them.

(e) *Requests for Authority*. Any Department not referred to herein and any Department established hereafter shall not have the authority to originally classify information or material under this Order unless specifically authorized hereafter by the President. Requests for such authority shall be directed by the head of the Department to the Director of the Security Information Oversight Office established by this Order, and shall identify the positions requiring the authority, the classification level required and present jusification for granting such authority.

(f) *Accountability for Classification*. Original classifers as designated under this Section, shall be held accountable for the propriety of the classifications assigned by them.

(g) *Exceptional Cases*. In exceptional cases when a person or Department not authorized to originally classify, originates information which is believed to require classification, such person or Department shall protect that information in the manner prescribed by this Order and implementing directives. The information shall be transmitted under appropriate safeguards to the Department having primary interest in the subject matter, or where such Department cannot be identified, to the Director of the Security Information Oversight Office, with a request that a determination be made as to classification.

SECTION 5. Classification Guidance and Duration of Classification

(a) *Requirement for Guidance*. Departments having original classification authority must issue classification guides. Such guides will be prepared at the earliest practicable time, but in any event prior to initial funding of a classified program, project, or plan. The guides must be reviewed by issuing authorities at least every two years. Guides must include *what* information should be classified; what the *level* of classification is; and, *how long* the information should be protected at each applicable level under the criteria for classification established by this Order.

(b) *Exceptions to Guidance Requirements*. Departments having original classification authority may request exemption from this requirement for specific programs, projects or plans by setting forth reasons for exemption and submitting them to the Security Information Oversight Office. That Office will determine whether the exemption will be granted and for how long. Appeals from the determination may be submitted to the National Security Advisor to the President whose decision will be final in such matters. Publication of these exemptions will made in suitable form.

(c) *Duration of Classification*. Except for the authority granted to heads of Departments pursuant to Section 8 hereof, the following limitations shall apply in determining the period during which an assigned security classification shall remain in force.

(1) Officials exercising original Secret and Confidential classification authority pursuant to Section 4 (b) and (c) hereof may assign any period not in excess of six full calendar years as the period during which information or material originally classified by them shall retain its assigned classification.

(2) Officials exercising original Top Secret classification authority under Section 4 (a) and heads of Departments designated under Section 4 (b) and (c) hereof may assign any period not in excess of 20 full calendar years as the period during which information or material originally classified by them or by original classifiers under their supervision or control shall retain its assigned classification. They shall exercise this authority with utmost restraint. In each case that they authorize classification beyond six years they shall in a guide issued under their authority, or by an original Top Secret classifying authority – who is so identified – set forth the reasons why the specific program, project, plan or the information is authorized to be protected beyond six years. If a guide is not issued, they shall include such rationale on all copies of the classified document containing the information.

(3) Original classification authorities shall, at the time of original classification determination, set a specific date or event for automatic downgrading or declassification. Such determinations will be reflected in guides or, in the absence of guides, on all copies of the documents. All such dates or events shall be as early as the national security interest will permit and shall be within the limitations established in (1) and (2) above.

SECTION 6. Identification and Marking

(a) *Required Information*. Each item of classified material shall show:

(1) One of the three levels of classification defined in this Order. No other terms, *e.g.*, "For Official Use Only," "Limited Official Use," *etc.*, shall be used as an identification of official information or material as requiring protection in the interest of national security, except as otherwise expressly provided by statute or

implementing directive.

(2) The office of origination

(3) The date of issue

(4) A date or event for declassification or review

(b) *Portion Marking*. Each classified document shall by marking or other means clearly indicate (1) each portion that is not classified and, (2), the level of classification of each classified portion. Heads of Departments may, with good cause found, seek exemption from this marking requirement from the Director of the Security Information Oversight Office. Appeals from adverse determinations may be made to the National Security Advisor to the President whose decision will be final in such matters.

(c) *Atomic Energy Markings*. Classified information and material, as decribed in Section 13, requires the additional marking "Restricted Data" or "Formerly Restricted Data" as the case may be.

(d) *Foreign Origin Markings*. Clasified information or material furnished to the United States by a foreign government or international organization shall either retain its original classification or be assigned a United States classification. In either case, the classification shall assure a degree of protection equivalent to that required by the government or international organization which furnished the information or material.

SECTION 7. Derivative Classification

Departments or persons who only reproduce, extract, summarize, or otherwise use information previously determined to be classified, shall not require original classification authority for the purpose of place or directing the placement of classification markings on new material – the classification of which is based solely on such previously classified source information. Persons who make the determination to apply classification markings shall, to the maximum extent practicable (by reference to current guides or other authority), verify the current need for classification and the level of classification of the information or material prior to applying such marking. They shall carry forward to any such newly created documents or material the dates or events assigned by the originator to the source material for declassification or review.

SECTION 8. Downgrading and Declassification

Downgrading and declassification of classified information shall be given emphasis comparable with that accorded to classification. The determination to downgrade or declassify shall not be made on the basis of the level of the original classification but rather on the expected perishability and loss of sensitivity of the information with the passage of time.

(a) *Authority*.

(1) Information or material may be downgraded or declassified by the official who authorized the original classification, by a successor in interest or capacity, or by a supervisory official of either. In this context, original classification guidance is expected to be a primary source of information for downgrading as well as declassification. To expedite and facilitate this process, heads of Departments shall designate officials at appropriate levels of command, knowledgeable of and responsible for the subject matter, to exercise declassification authority and resolve doubts or conflicts regarding interpretation of guidance issued by such heads of Departments.

(2) The Director of the Security Information Oversight Office shall have the authority to downgrade or declassify information or material considered by his office in the exercise of its appellate function as described in Section 11 of this Order. Further, in the exercise of his oversight responsibilities, in any instance that the Director determines that continued classification would constitute a violation of Section 3 (b) of this Order, he will downgrade or declassify the information in question. These declassification decisions shall not take effect for a period of ten working days, during which the head of the affected Department may appeal the decision to the President through the Assistant to the President for National Security Affairs.

(b) *Downgrading Action*. Information or material classified under this or prior Orders shall be downgraded to a lower level when, upon review for any purpose by those authorized in (a) (1) preceding, the information or material is found to require protection at less than the originally assigned level. Downgrading action will be reflected by changing the markings and reassigning a date for review or declassification. Holders of downgraded material shall be notified by the downgrading official unless the action is taken as a result of published guidance.

(c) *Declassification Action*. It is an intent of this Order to establish a program whereby information or material under the exclusive classification jurisdiction of the United States shall, in general, not remain classified for more than 20 years. This program will be effected as follows:

(1) *New Material*. All official information or material classified on or after the effective date of this Order shall be declassified or reviewed for declassification in accordance with the dates or events specified by original classification authorities pursuant to Section 5 (c). Treatment of derivatively classified information is covered in Section 7.

(2) *Old Material*.

A. Information or Material less than 20 years old. Information or material classified before the effective date of this Order and already determined to be declassified in 20 years or less, and so marked, will be declassified in accordance with such determinations unless such information or material is identified in guides or guidelines issued under the authority of the heads of Departments described in Section 4 (a), (b), and (c), for a later review, or guides or guidelines establish an earlier date for declassification.

B. Information or Material 20 or more years old. Information or Material which was classified before the effective date of this Order that is marked with a date or event directing declassification later than 20 years after its issuance, will be reviewed for declassification as required for use, or to reflect determinations made by heads of Departments described in Section 4 (a), (b), or (c), or as required in current guides or guidelines.

(3) *Systematic Review of Permanently Valuable Records.* To conserve the Government's declassification review resources, systematic review of information or material that has remained classified for 20 years or more will not be required, excepting for that information or material which is a part of the permanently valuable records of the Government as defined in 44 USC 2103. Heads of Departments shall order the review of all security classified records 20 years old or older which are held in storage areas, for possible disposal. Records which are found not to be scheduled for disposition shall be scheduled for review immediately. In the conduct of this review, the declassification guidelines issued by heads of Departments as prescribed in (d) below, shall be applied. Only the heads of Departments designated in Section 4 (a), (b), or (c) — or their designees — shall be authorized to continue — beyond 20 years — the classification of information or material which, after review, is determined to require continued protection in the interest of national security. In such cases, a date or event for declassification will be set, or a date for subsequent review, not to exceed ten years, will be established.

(d) *Guidelines for Declassification.* Within 180 days after the effective date of this Order, heads of Departments identified in Section 4 of this Order shall, in consultation with the Archivist of the United States, issue classification guidelines applicable to information or material under their respective jurisdictions that has remained classified for 20 years and shall disseminate these guidelines, making them available to any holder of that information or material. The guidelines shall specifically identify those items or categories of information or material which — because of their continuing sensitivity and importance to the national security interest — cannot be automatically declassified, but must be reviewed shortly before their 20th anniversary to determine the need for continued protection beyond 20 years. That information or material not identified in the guidelines as requiring review shall be automatically declassified at the end of 20 full calendar years from its date of origin.

(e) *Mandatory Review.*

A. All information or material classified under this or predecessor Orders shall be subject to declassification review by the originating or responsible Department upon request of a Department, an employee of any Department, or a member of the public provided the request describes the material sufficiently to enable the Department having custody to locate it with a reasonable amount of effort. Non-federal records (*e.g.*, Presidential materials, donated historical materials as defined in 44 USC 2101, and other classified materials in a non-federal repository) which are less than 10 years old may be exempted from the provisions of this section.

B. After review, the material — or a reasonably segregable portion thereof that no longer qualifies for security protection — shall be declassified and released, unless it is determined that there are overriding reasons for withholding the information under other applicable exemptions of the Freedom of Information Act or the Privacy Act (5 USC 552 as amended).

C. The head of each Department shall designate an office to which requests for mandatory review for declassification may be directed, and publish this fact in the Federal Register.

D. The President, through the Security Information Oversight Office, will issue procedural instructions for processing initial requests and appeals from denials.

(f) *Departments Without Current Classification Authority.* The provisions of this Order set forth in this Section relating to the downgrading or declassification of material shall apply to Departments which, under the terms of this Order, do not have current authority to originally classify information and material, but which formerly had such authority under previous Orders. The authority may be exercised only on material originated by such Department and under their then exclusive classification jurisdiction.

SECTION 9. Transfer of Material

(a) *Official Transfers.* In the case of classified material officially transferred by or pursuant to statute or Executive Order in conjunction with a transfer of function

and not merely for storage purposes, the receiving Department shall be deemed to be the originating Department for all purposes under this Order including downgrading and declassification.

(b) *Disestablished Departments*. In the case of classified material that (i), originated in a Department that has since ceased to exist, and (ii), has undergone no official transfer as described in (a) preceding, any Department in possession may, for the purpose of this Order – in particular, for the downgrading or declassification of such material – take action as if it were the originating Department, following consultation with and consent by all other Departments having a recognized interest in the subject matter. Having taken such action, the Department shall be deemed the originating Department.

(c) *Material in Archives of the U.S.*. Classified material transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded or declassified by the Archivist of the United States in accordance with and to the extent defined by (i), this Order, (ii), directives of the President issued through the Security Information Oversight Office, or (iii), pertinent regulations and declassification guidelines of the Departments.

(d) *Presidential Materials*. After the termination of a Presidential administration, the Archivist of the United States shall have the authority to review, downgrade or declassify material which was classified by the President, his White House staff, special committees or commissions appointed by him, or others acting in his behalf. This authority shall be exercised only after consultation with the Department having primary subject matter interest.

SECTION 10. Safeguarding

(a) *Policy Directives*. The Director of the Security Information Oversight Office shall, with the approval of the President, issue directives which shall be binding on all Departments for uniform standards for access to classified information and for the protection of classified information from loss or compromise. Such directives shall conform to the following policies:

(1) No person shall be given access to classified information or material unless such person has been determined to be trustworthy and unless access to such information or material is necessary for the performance of that person's duties. To provide a more complete basis for a determination of trustworthiness, access to and obtaining of criminal justice information from Federal, State and Local law enforcement agencies is authorized as it pertains to personnel investigations under this Order.

(2) All classified material shall be appropriately and conspicuously marked to put all persons on clear notice that the material is classified and that it is National Security Information.

(3) Classified information and material shall be used, processed, stored, transmitted and destroyed only under conditions which will prevent access by unauthorized persons and dissemination to unauthorized persons.

(4) All classified information or material disseminated outside the Executive Branch shall be properly protected.

(5) Appropriate controls for classified information or material shall be established and maintained commensurate with the level of classification. Such controls shall be uniformly applicable to all holders of the information or material.

(6) Classified material no longer needed will be promptly destroyed in accordance with applicable statutes and regulations.

(b) *Secrecy Agreements*. Heads of Departments may authorize the use of a secrecy agreement applicable to employees – military, civilian and industrial – as a pre-condition of access to all classified national security information and material. The Security Information Oversight Office shall, in coordination with Departments, develop a uniform secrecy agreement which heads of Departments may adopt. Existing secrecy agreements need not be re-executed.

(c) *Special Access*

(1) Special Access programs may be created or continued only by the head of a Department, personally and in writing. The authority to approve a special access program may not be further delegated. Special access programs pertaining to intelligence sources or intelligence methods may be created by or continued by the Director of Central Intelligence personally and in writing.

(2) Special access programs may be created or continued when:

A. The importance and sensitivity of the information involved necessitates the imposition of special requirements with respect to access, distribution and protection.

B. Normal safeguarding procedures are determined not to be adequate.

C. The program requiring such special controls can be kept in reasonable size, and the head of the Department establishes special internal controls to ensure against unwarranted or unreasonable growth in the numbers of persons requiring access.

D. The sensitivity and importance of the information fully warrants the additional costs involved.

(3) All special access programs created or continued shall be:

A. Reported to the Director, Security Information Oversight Office.

B. Reviewed annually by the head of the Department or the Director of Central Intelligence, as appropriate.

C. Terminated after three years from the date of approval unless specifically continued for an additional term which shall not exceed three years.

D. All special access programs in effect at the effective date of this Order shall be reviewed for termination or continuation within 180 days. The identification of all programs terminated or continued, together with the length of the additional term, shall be reported to the Director, Security Information Oversight Office.

(d) *Historical Researchers and Former Officials*. The requirement in this Section (paragraph (a)(1)) that access to classified information or material be granted only as is necessary for the performance of one's duties shall not apply to persons outside the Executive Branch who are engaged in historical research projects or who have previously occupied policy-making positions to which they were appointed by a President. *Provided*, however, that in each case the head of the originating Department

(1) Declares in writing that access is consistent with the interests of national security

(2) Takes appropriate steps to assure that classified information is not disclosed by the researcher without prior review and approval. In the event of potential publication, that the information has been reviewed, declassified, and approved for public release.

(3) Takes reasonable action to ensure that access is limited to specific categories of information over which that Department has classification jurisdiction.

Access granted a former official by reason of his having previously occupied a policy-making position shall be limited to those papers which such former official originated, reviewed, or signed while in public office.

SECTION 11. Implementation and Review

Overall responsibility for policy direction of the program established pursuant to this Order shall rest jointly with the Director of the Office of Management and Budget and the Assistant to the President for National Security Affairs. The responsibility for monitorship and implementation of the program is vested in the Director of the Office of Management and Budget.

(a) *Oversight Office*. There is hereby established in the Office of Management and Budget a Security Information Oversight Office, hereafter referred to as the Oversight Office. The Oversight Office shall be headed by a full-time Director. He shall be appointed by the President and authorized to maintain a permanent staff. The Oversight Office shall:

(1) In accordance with procedures to be established by its Director, oversee Departmental actions to ensure compliance with the provisions of this Order and implementing directives.

(2) Consider and take action on complaints and suggestions from persons within and without the Government with respect to the general administration of the Order, including appeals which involve the declassification of material which is ten or more years old.

(3) Develop and promulgate standards for uniform application throughout the Executive Branch for the scope of investigation and adjudication of results, including due process safeguards, to determine trustworthiness of individuals for access to Secret and Confidential information, Top Secret and especially sensitive material such as intelligence sources or methods, cryptologic, and all other information currently designated as sensitive compartmented information.

(4) Develop, in coordination with Departments, directives required for effective implementation of this Order.

There is also established an Interagency Security Information Advisory Committee which shall be chaired by the Director of the Oversight Office and shall consist of representatives of the Departments of State, Defense, and Justice, the Energy Research and Development Administration, the Central Intelligence Agency, the National Security Council Staff, and the National Archives and Records Service. The Interdepartmental Committee shall meet at the call of the Chairman and shall act in an advisory capacity to him in all matters related to effective implementation of this Order and implementing directives.

(b) *Departmental*. To promote the basic purposes of this Order, the head of each Department originating or handling classified information or material shall;

(1) Submit, prior to the effective date of this Order, to the Oversight Office for review a copy of the regulations it proposes to adopt pursuant to this Order and implementing directives. Subsequent changes in Departmental Regulations shall also be forwarded to

the Oversight Office for review.

(2) Publish in the Federal Register those regulations and changes issued in implementation of this Order that have been reviewed by the Oversight Office, to the extent that they affect the general public.

(3) Designate a senior staff member to serve as a Departmental monitor, who shall conduct an active monitorship program for the purpose of ensuring compliance with and implementation of this Order. The Departmental Head shall also designate a senior staff member who shall chair a Departmental Committee which shall have authority to act on all suggestions and complaints with respect to the Department's administration of this Order, including appeals from denials of requests for declassification review.

(4) Establish a continuing program to familiarize Departmental personnel and others authorized access to classified information and material with the provisions of this Order and implementing directives. There shall also be established and maintained active security orientation and education programs to impress upon all persons their individual responsibility for complying with the provisions of this Order with vigilance and care.

(5) Assure the preparation and promulgation of security classification guidance to facilitate the identification and uniform classification, downgrading, and declassification of information requiring protection under the provisions of this Order.

(6) Develop and promulgate downgrading and declassification guidelines in accordance with Section 8 hereof.

(7) Take necessary action to assure that: (i), a demonstrable need for access to classified information and material is required from individuals prior to the initiation of administrative clearance procedures, and, (ii), the number of people granted access to classified information and material be reduced to and maintained at the minimum consistent with operational needs.

(8) Conduct a continuing review of safeguarding practices and procedures to ensure that national security information and material is protected to the extent required by this Order and that they are consistent.

(9) Submit to the Oversight Office :(i) on an annual basis, a listing of those officials within the Department who have been designated in writing as original classification authorities; (ii) on a semi-annual basis, such oversight progress reports as the Director of the Oversight Office determines to be necessary; and (iii) such other information or reports as the Director may require for administration of the program established herein.

SECTION 12. Administrative Sanctions

(a) Any officer or employee of the United States who knowingly or willfully classified or continues the classification of information or material in violation of this Order or any implementing directive, or willfully or knowingly and, without authorization, discloses classified information or loses classified material through gross negligence; or, as determined by a head of a Department, violates this Order or an implementing directive, shall be subject to adminstrative sanctions as appropriate. In any case in which the Oversight Office finds that unnecessary classification or overclassification has occurred it shall make a report to the head of the Department concerned so that corrective steps may be taken.

(b) The head of each Department is directed to take prompt and stringent administrative action whenever a violation as provided in paragraph (a) preceding occurs. Sanctions may include, but are not limited to, reprimand, suspension without pay, removal, or other sanction in accordance with applicable law and Departmental regulations. Additionally, heads of Departments shall immediately inform the Department of Justice of any case in which a violation of criminal law may be involved.

SECTION 13. Atomic Energy Material

Nothing in this Order shall supersede any requirements made by or under the Atomic Energy Act of August 30, 1954, as amended. "Restricted Data," and material designated as "Formerly Restricted Data," shall be protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and the regulations of the Energy Research and Development Administration.

SECTION 14. Enabling Data

(a) Executive Order No. 11652 of March 8, 1972 as amended by Executive Orders No. 11714 of April 24, 1973, No. 11862 of June 11, 1975 and all implementing directives issued pursuant to Executive Order 11652 are superseded as of the effective date of this Order.

(b) This Order shall become effective on January 1, 1978.

(Ed. Note: The dates shown in this draft – submitted on 5 August – are not current. At the time of preparation it was expected that the Order would issue under a date of 15 September. As we go to press the date is uncertain. The most recent coordination draft indicated an effective date of 1 March 1978.)

Practical Exercise

FROM CONCEPT TO MANUFACTURE

Board of Directors
National Classification Management Society

The following presentation format was retained for several reasons:

- It can be illustrative of a way to proceed in conducting what is a rather elaborate and difficult series of exercises
- Points relating to facets of problems can be emphasized in order – despite written instructions – that participants don't become lost
- A lightening effect can be achieved (we believe that we were moderately successful) if two persons well familiar with the points to be covered and the topic can "free form" the exchange.

In the interest of reducing repetition, only the first names of the co-moderators will be used; James J. Bagley, the Seminar Chairman, and Jack A. Robinson, the Program Chairman.

Jim: As we begin, I might mention that there was a question just a moment ago about whether the lights on the platform should be on or off. Frank Larsen made a comment to which I thoroughly subscribe. If the lights are on, we become a better target; but if they are off, one might miss.

Jack: Well, Jim, I'm not going to use the mike because with what I have to say, I prefer not to be heard too well. But, we have been fiddling with this problem for a bit, haven't we?

Jim: Oh, I would say so.

Jack: When the guys and gals are exposed to it, they will think both of us have lost our cotton-pickin minds. Shall we, however, tell them why?

Jim: Well, the example is kind of like this. We said if there was going to be an exercise in kind of contradistinction to the three pigs, it should be realistic. And, to be realistic one should follow the process of what the services issue as a requirements document. Originally, you might remember, that both the most recent Secretary of Defense Statement and the most recent Director of Defense Research & Engineering Statement, spoke of the critical needs in land warfare, and you've also heard here that some of the more critical problems are in land warfare.

Jack: May I ask, Jim, if you would permit me to quote from, in fact, Dr. Currie's statement . . .

Jim: Of course.

Jack: . . . It was issued as part of his "Swan Song" relating to current technology, as he was leaving DoD in 1977. It relates also, for instance, to comments made by Mr. Liebling relating to DoD involvements and assessments concerning technology. I quote: *"It is in the area of land warfare systems that I am most immediately and urgently concerned. The Soviets in many cases are widely deploying technology* **now** *for which we will not have roughly comparable counterparts until the early or mid 1980s."* That concern was echoed in a similar statement by the Chairman of the Joint Chiefs of Staff – also in 1977. That's part of the rationale.

Jim: So what we did, therefore, is to develop a land warfare exercise. Back in my dim, dark past, I was a tanker . . .

Jack: Is there a "D" on that?

Jim: No comment. Ignoring the interruption, I had an affinity for armored vehicles. So, I said to myself, if there is going to be, as the various important people have said, a critical problem in land warfare, then obviously, the tank remains a very important part; what would be the kinds of improvements needed for a tank to become a viable, really viable, weapons system. So I postulated some improvements.

As an aside, it's kind of interesting that there was a joint meeting of NCMS and ASIS a few weeks ago in which I talked about this exercise and our approach to provide realism. Some of the people from ASIS, also armor oriented officers, descended on me and asked what I had used as a basis for the exercise. So, I said that I could see nothing wrong with a tank having a first round hit capability at six kilometers and under all weather conditions. Further, I could see nothing wrong with secure communications in a tank; that it was technically feasible now.

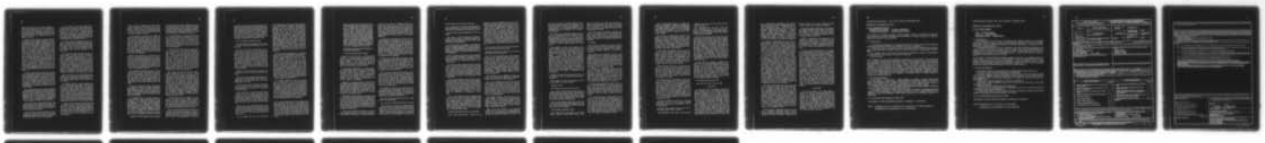
Jack: But Jim, you are forgetting an important part of the problem of getting this show on the road. The participants may be interested in the fact that the last piece of paper that they are going to get as part of this package, I got from the printers this morning – just to give them an idea of the time frame under which we have been operating. As you commented previously, however, we have a new bag of tricks here. What, in fact, have they got on their desks?

Jim: First, you have the new DD Form 254, an

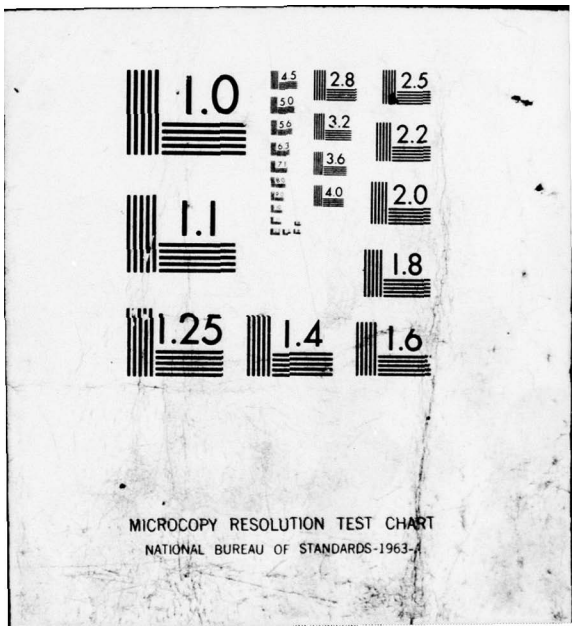
AD-A049 251 NATIONAL CLASSIFICATION MANAGEMENT SOCIETY ALEXANDRIA VA F/G 5/1
CLASSIFICATION MANAGEMENT. JOURNAL. VOLUME XIII, 1977. PAPERS F--ETC(U)
1977

UNCLASSIFIED NL

2 OF 2
AD
A049251



END
DATE
FILMED
3-78
DDC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
8.0
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

NCMS presentation, that has been approved recently. With the exception of item 12, and there's a very careful remark saying so. This will be the document published I would guess sometime in the fall. Bob Green from Headquarters Defense Logistics Agency, Directorate for Industrial Security will address that point.

Second, you have a "piece" of paper containing the extracts of the changes proposed to the Industrial Security Manual (ISM) to accompany the new DD 254. What you're seeing is something brand new which was virtually taken off Joe Liebling, Art Van Cook, and Tom O'Brien's respective desks. They agreed to our using it. Parenthetically, we were aided and abetted by Bob Green and Colonel Pruett, as you might imagine but wouldn't know. To be certain that it was not imagined to be "for real" we had it printed in blue. It also says *This form represents that approved at DASD (SP) and ready for issue subject to the note contained in item 12.* It also says *DD Form 254 (Provisional).* But to the best of our knowledge, this is *it*. So your Society is attempting to provide advanced – by several months at least – exposure to new requirements. Please, when you have the opportunity, read the fine print *carefully* and you may be able to do some advanced planning that will help you and your office.

Turning to other pieces of paper that you have. Two are Capability Category 78X and 78XX. We were proceeding, Jack and I, on the basis of Operational Capabilities Objective documents put out by the Army as described in existing Army Regulations. Lo and behold, we found out that the Army, as a result of a DoD directive (at least in part) has republished all of its known objectives in a new format called the Scientific and Technical Objectives Guide (STOG).

Jack: Correction please. AR71-9 which specified and established the Operational Capability Objectives has not yet been reissued. We are in advance of its publication also. The Scientific and Technological Objectives Guide is being published, but the Army Regulation has not yet been issued to establish it. You are, if you are associated with the Department of Army, slightly in advance in this context also.

Jim: By the way, we feel good about this. This follows absolutely the format of the STOGs. The systems that we have postulated are presented in that format and are in the kinds of words and the kinds of justification included.

Jack: Of course, I will call attention, should it be necessary for this Society, that this is an hypothetical system characterized "way out," classified for exercise purposes only *as you will note please.*

In this context, by the way, yesterday Dr. Church had an immediate sinking feeling when I gave him the first two papers. He said, "That's not for real, is it?" I said, "no sir." The paper does say "Classification Marks are For Exercise Purposes Only." But, in that frame of reference, unless we, in fact, practice the determinations and decision making process that is needed, *MARKING will not have* the importance that is needed for all of us.

So, we're playing two games. We're playing a game of determinations and decision making processes; and you will be playing several roles which we'll describe later. But we're also playing a brand new game on "what do you do without the DD Form 254c?" Shall I leave the description to Bob Green, Jim?

Jim: By all means. What I am about to say is, of course, subject to change by Bob, and certainly within his prerogative and authority. We felt it would be absolutely inappropriate for us, Jack or me, to describe the changes and approach. We have taken a piece of paper as it is and using that *piece of paper* as we read it. But I would ask, Bob Green to describe the changes that are forthcoming in the DD Form 254. I emphasize that it has been approved with the exception of Item 12 (as of 10 May 1977). He can tell you better the publication date. (Ed.Note. Subsequently the existing Item 12 was approved for inclusion in the revised DD Form 254)

Jack: All of you I'm sure know Bob Green, Head of the Industrial Security Programs Division of The Executive Directorate, Industrial Security, of the Defense Logisitics Agency. We are pleased that he can join us.

Mr. ROBERT GREEN: I didn't expect to be a part of your program, nonetheless, I'm delighted to be here. When Jack called me about a month ago and asked me what I thought about the possibility of getting an advanced look at the final approved format of the DD 254 for purposes of this workshop, I thought it was a very excellent opportunity for us to get an advanced training seminar working. Between the two of us talking with Art Van Cook in Mr. Liebling's office, we were able to get permission to take the DD 254, even though not formally approved at this point for use as a training vehicle.

I know you're all interested in the rationale and the details of many of the changes that you will find in the new 254. I don't want to belabor the point. Last July at the Sheraton Harbor Island in San Diego, I gave a reasonably detailed rundown on the changes and the rationale behind them. You'll find those remarks in your proceedings from last year's seminar.

But, I want to emphasize the primary thrust behind the changing of the DD 254 at this point and time. Number one, and the foremost reason, frankly is that the old DD Form 254c checklist did not work. It did not convey classification guidance from the User Agency to industry.

A few years ago we came up with a 254c, the intent of which was to encourage you in addition to those little Xs and check marks you put on the form to provide additional narrative guidance which would be far mor understandable than a check mark against a subjective title. Unfortunately, that didn't work too well either. Apparently the people who were responsible for preparing that 254c felt that when they put a check against a subjective title, since *they* understood what they meant, everybody else would understand it too; and there was no need for any narrative dissertaion.

Based on the comments we received from the field and the continuing complaints from industry and the continued problem primarily from the government, the initiators of 254s, we had some discussions with OSD. We decided that the only solution was going to be to cast the 254 essentially in the same format as User Agencies are required to prepare for their own departmental classification guides – that is a straight narrative guide.

Now, that doesn't mean that you have to write a narrative guide for every 254, because you should receive the classification guide that has been prepared by the User Agency with your projects and with your 254s. That is your narrative guide. It's only when there is no project guide written by the User Agencies despite DoD regulations that there would have to be a narrative written exclusively for a 254.

The obvious end result we hope for is that there will always be a DoD User Agency classification guide prepared in advance of the 254 issued with a new or amended contract. There will be no need to rewrite or to originate any narrative guidance to go with that classification guide. That was the primary thrust of the change.

The secondary thrust – we have a mission in DCAS, the Office of Executive Director for Industrial Security – of monitoring and reporting to DoD the effectiveness of the DoD and User Agencies' implementation of the Classification Management Program as it affects the contractor. To do that we have established an ongoing management information system. It's computerized. It depends on input, in many cases, directly from a DD Form 254. So, some of the information you will see in the new 254 is there for management information purposes.

I recognize the basic objection that some people have raised that the 254 is supposed to provide classification guidance and that should be its exclusive and dedicated use. But I counter that with the suggestion that anything that improves the program, the Classification Management Program, is appropriate information to be included in the 254.

The only information I can give you as to when the new 254 is going to be available for use will have to be "waffled" a bit. It is currently in Mr. Liebling's office. It has been the full government/industry coordination route. It is current in the internal DoD coordination which is the last step prior to getting an approval to publish in the Industrial Security Program.

I would like to say that we'll get it back tomorrow or next week or next month. It depends on what problems may be encountered internally within DoD. I do not anticipate at this point and time – and we have been in almost daily touch with Art Van Cook – any change in the principal substance of the DD Form 254. I think what you will see in the months to come as the finished document will be essentially the same as you see it today. The format may change. Jack, obviously from the rough copy we gave him, had to take some formatting liberties. But the form will be essentially the same as you see it. Considering the available draft, the product is excellent.

We are also anxious to see on the street, just as anxious, perhaps, as some of you are – maybe you're not so anxious; maybe I'm anticipating – to release this form to the school at the Defense Industrial Security Institute (DISI) so that they can start cranking this new format, new content, and new concept into the Information Security Training courses that are presented. You may be interested to know that over the past year DISI has conducted ten resident courses on Information Security and eight field extensions. It's my understanding that in this fiscal year, there will be even greater exposure to Classification Management and the DD254 in that Information Security Management Course. Many of you have attended. I would certainly encourage all of you to do so.

I am here really only as an observer. I'm very anxious to see how this new format is going to work out in practice. I intend to be here with you for the rest of the afternoon and the balance of your practical exercise tomorrow morning. If any of you have specific questions that you'd like to discuss with me, I hope you will feel free to do so.

Jack: A real point which Bob just mentioned and Jim before, let me repeat. Questions with respect to absolute interpretation of the changes as written in the forms you have or the form itself, obviously we cannot answer. The interpretation as you see it

throughout this exercise, and I do hope that is the reason why Mr. Green with Colonel Pruett's approval, was kind enough to agree to be present and to field those questions that may become important as you work through the exercises. It is a very important contribution for which we are grateful indeed. So they will do that. If *you* think the words say one thing and we have apparently interpreted them to be another, the arbiter for the case is Mr. Green.

So, Jim, what are we going to do now?

Jim: Now we will start the process. As soon, that is, as some irreverent wag commented, as we find *the strip.*

Jack: We were going to say that right now you need to read. You need to read for two very important reasons. None of you have seen these changes nor have you seen this version of the DD Form 254. To work through this exercise requires that you become at least somewhat familiar with them because the words make a difference, and the words on the form are different from those to which you have become accustomed. If you have not become accustomed to using them, it still means the same thing – you *need* to become accustomed to using them. So, reading is in order, and we have planned to provide the time.

However, Jim, what are they *really* going to do? They may not want to know, but you'd better tell them.

Jim: As Jack said, read the problem because it is fundamental to understanding. Then when this is done, there will be four roles that you will play. *EMPHASIS* – four roles.

First, you will be the Headquarters issuing guidance. Second, you will be a Systems or Material Command (SysCom) and prepare a prime contractor DD Form 254.

Now, at this point it should be mentioned that to save time we are cutting the process. We are avoiding many of the procurement actions like Requests for Proposals (RFPs), Requests for Quotations (RFQs), Invitations for Bid (IFBs), and such. We are assuming that all of this has been accomplished and that a Prime Contractor has been selected.

Thirdly, then, you will become the Prime Contractor issuing a subcontractor DD 254 for a total subsystem. And lastly, you will be the poor joker at the end of the totem pole – the subcontractor who says to his boss, "Yeah, boss, this is what we're going to do."

Let me repeat: first, you're, in this case, the Army Headquarters. You are then issuing a directive to the Army Materiel Command. As the Materiel Command you will do whatever coordination is necessary and you will issue the Prime Contractor DD Form 254. You will take action as a Prime Contractor and finally as the subcontractor. Throughout this process, there will be explanatory things. Frank Larsen (from Department of Navy Headquarters) will talk to you about the role that a Headquarters generally plays. Carolyn Meadows (from Headquarters, Naval Air Systems Command) will talk about the kinds of things at a Systems or Material Command that must be done – in this case aided and abetted by a member of the Army system whom Jack will introduce later. Finally, members of the Board representing major industry, will give observations on their actions when receiving such a document.

Jack: Before they begin reading, Jim, it might be well to comment that Headquarters representation is reflected in two pieces of paper that they have – namely Capability Catergory 78-X and 78-XX. We've commented that this is cast in an Army frame. As you read more into it you will realize that the systems involved in this application do have application across the three services. The Headquarters' consideration is essentially similar for all three services. The words may differ but the process and consideration is essentially the same. You may remember that this is so from the comments of the three Chief Scientists whom you heard yesterday regarding what's to be protected. For that reason, it might be appropriate to ask Board Member Frank Larsen to make a few comments about the process of decision-reaching as CNO views it.

Mr. FRANK LARSEN: On very few occasions has one confronted so many friendly and hostile faces! Jack and Jim have asked me to very briefly orally paint for you a picture as to what happens at the genesis of this problem of a new program and classification guidance to provide a little backdrop for the exercise. In this case, a weapons system; but really to talk about how we identify that information that requires protection, to see what the object is, as we do. Classification guidance then can accompany an approved program at the very outset, so that everybody operates from the same base.

Now I see some skeptical looks in the audience; and, I fully understand that there is a gap between what Headquarters does and what the users finally get – sort of a credibility gap, perhaps. It's probably like the man that was pursuing a title search on his property. He just couldn't believe that the government only had records on the Louisiana Purchase dating back to 1803. So, under the Freedom of Information Act, he persisted in knowing more. Finally, he got this letter, and I quote:

Please be advised that the government of the United States acquired the Territory of Louisian by purchase from the government of France in 1803. The government of France acquired title by conquest from the government of Spain. The government of Spain acquired title by the discovery of Christopher Columbus, an explorer, and resident of Italy, who by agreement concerning the acquisition of title to any land he discovered, traveled under the sponsorship and patronage of Her Majesty, the Queen of Spain. The Queen of Spain received the sanction of her title by consent of the Pope, a resident of Rome and an *ex officio* representative of Jesus Christ.

Jesus Christ was the son and heir apparent of God. God made Louisiana.

I trust this complies with your request.

Believe it or not, we try to – at the very earliest opportunity – consider everything that is applicable to the new program. And while the mechanics may be slightly different, I'm sure that all the services and agencies involved in this classification process go through similar procedures. So let me just name one to give you an idea of how the ball gets rolling.

An Operational Requirement or a Specific Operational Requirement (SOR), or whatever, is decided by the policy makers and the operators to be a valid program to pursue in order to provide a new weapon in the hands of our fighting forces. A requirement – hopefully one that advances the state of the art far enough so that we will have a net advantage in the event of a confict – is established.

Obviously, as we heard yesterday, the scientists who are familiar with technology have an input in terms of making that kind of determination and an overall classification usually is assigned. It is formalized at the very highest levels into a document with an overall classification that their Project Office has assigned to it and the process for funding the project for approval through to the Congress is started.

Simultaneously with that action, the project comes to a central point in the Department of the Navy with a request that classification guidance be developed in more finite terms. So we have a requirement. We have some idea of the magnitude of the problem, and the level of classification which has already been arbitrarily assigned. We are not experts in the technology; but we do have some other assets that we utilize in the development of the guide itself.

First, we ask our foreign intelligence to provide a Net Technical Assessment of what the Russians or other potential foes may have in this same area as the requirement. We receive an intelligence estimate relative to their state-of-the-art in the field, their knowledge of the technology required for the system. We make a decision on what is it that we really need to protect? As we heard yesterday, it is pointless to try to protect something that is already common knowledge. Application, maybe, but certainly not the technology which may be well known to our potential adversaries.

We write also to somebody else. We write to our counterintelligence people because they can tell you what an adversary is interested in trying to get from us. Now we know they get the technical publications; they get the *The Congressional Record*, so they have a good start on collecting information. But are they spending their good, hard-currency money for clandestine-type operations? The response gives us a feel for whether this particular subject matter is important to them. If it is, it gives us a hint that perhaps we ought to hang on to the information at least for a while, until we get more finite guidance.

We also go to our Naval Material Command and ask for a technological input from the viewpoint of the procurement activity. We take all the pieces of information and then we go to the "good book" like we're supposed to do and we start talking about what is it we can protect, how vital are the specifics of the information in terms of causing damage to the effort or damage to the national security?

Then we draft a guide and send it back to the Project Office saying, "here's our recommendations." More often than not it's approved; but at least one thing has been accomplished. Incomplete though it may be at that point and time, a thing called a classification guide is married to the project for everybody to use as a base point for classification. That usually is the way it is done, and it's being done more today than it ever has been before.

Jack: Thank you Frank. So, as Jim said, you are now Headquarters. The decisions with respect to a Headquarters, which follow from an activity such as Frank has described, are reflected in the classification assigned to the respective paragraphs in each of the two 78-X and XX documents before you.

Now we will give you what we will term a "quiet time" of 15 or 20 minutes.

Jim: That's for the whole bag of papers you have.

Jack: Of course. There are a few terms that we have used that can differ in interpretation. EMP is one that many know – we are using it in the sense of *Electromagnetic Pulse*. We have used also LPI. It has, unfortunately, multiple different meanings. In this instance we are using it as *Low Probability of Intercept*, in a

communications sense rather than a laser sense.

Jim: I believe all of you should note that there are some new definitions in the DD Form 254 itself for which there is an explanation in the glossary of terms.

Question: Please explain paragraph 5 of 78-X and 78-XX.

Jack: That is a new Army approach to establish a priority list piece by piece of items contributing to the attainment of the objective in the order of their needed sequence of accomplishment.

Jim: You'll notice, for example, on the header of 78-X that strategic communications, tactical communications, computer applications, and communications security, are included. Within that framework, they are prioritized in orders of technology objectives that need to be addresssed.

Jack: To simplify the problem, we have established that the priorities established in paragraph 4 are the same for paragraph 5 – clearly, this would not be true uniformly, and, in fact, much further detail is commonly found.

Jim: Also, we had to consider the risk of having to classify the whole damn document which we could not, of course, do. I think you should note also that some of these things are very, very long range which was intended. To have LPI communications in a tank is a bit far-fetched, although it's theoretically possible. To operate on a first round hit capability at a range of six kilometers, all weather, is also long range, in either of two senses.

But you might remember from Dr. Church's, presentation yesterday, he spoke of these kinds of things in his paper, such as the need for good communications. Now what he didn't say obviously is the fact that one of the important lessons from Vietnam is that we have very poor secure communications discipline. Another thing, which is also kind of implicit, is that we try to make new developments "idiot-proof," or "soldier-proof," or "sailor-proof" or "airman-proof," and so forth.

There is also introduced into this something which is very new and which may happen, probably in the next 15 years, and that is electronic destruct rather than physical destruct. I'm talking about the destruction of critical electronic components. This is entirely feasible. Although I emphasize that there is nothing in today's technology which will accomplish this, regardless of what you might think. It is not now possible; nor is it accepted doctrine today.

Question: What does FSC mean on the DD 254?

Jack: Federal Supply Code, I heard from the audience. In fact, that is indeed correct. I also tell you another little element. Most of you receive, if you are a contractor and this applies only to contractors, once a year a hunk of paper which is obviously from a machine printout which has a lot of data on it concerning your outfit – its current status, when you were cleared, when the clearance was updated, your address, *etc*. There are some other columns in it in which are various bits of information. One of these, and I think it is column eight, is called Federal Activity Code, and that translates to Federal Supply Code in these terms. I still have a small element of problem with respect to my own organization in that it seems to be impossible to decide which among several is the one.

Are you about ready for the first real operational step? Or do you need a little more time?

Question: Where do you find the list of Federal Supply Codes, or whatever they are?

Jack: You do not find the list of Federal Supply Codes. They are individually identified. You need to know them as a "person" being a contractor or you need to find them out if you are DLA (from your computer listing). If you are a User Agency, I guess you call DLA and find out and if you are a contractor trying to arrange for a subcontract – you ask. Bob will have to answer further details relating to that question. As respects the DoDAAD numbers, they are published (Department of Defense Activity Address Directive, which includes a specific number assigned to DoD procurement activities).

Jim: Illustrative of the DoDAAD numbers, the Office of Naval Research is N00014; NRL is N00173. In the Army it's four letters and two digits, *etc*.

Jack. Let me suggest that as far as FSC and DoDAAD numbers are concerned, they are not important to this exercise. The reason we used them is because they will be required and you will have to cope with them later. We tried to follow the instructions as we could understand them, so that you would have an example that you could refer to later. Bob Green may have a few observations that he could offer. Would you care to comment, Bob?

MR. ROBERT GREEN: The FSC number is controlled basically by the government contracts administration. There is an FSC number assigned to every contracting facility that does procurement with the federal government. Within the DoD the numbering system is controlled by Defense Logistics Supply Center at Battle Creek, Michigan.

When we go into a facility to do an additional facility survey for clearance in the Industrial Security Program, the Industrial Security Representative will ask, "Do you have an FSC number?" If you say, "No,

I do not," he will go to DISCO. DISCO will go to Battle Creek and the facility will be assigned a permanent FSC number. It consists of five characters – five numeric figures if it's a manufacturing facility, and an alphanumeric set of five characters if it is a nonmanufacturing facility.

The number is for identification purposes only. It's used a lot of different ways with respect to government procurement. We use it, if you will, in the Industrial Security Program because our classification management programs are now computerized. And it's much easier for us to handle with a five character set of figures to identify a specific facility in our computer.

The DoDAAD, is a number that is assigned to DoD activities. However, there are some contractors now who do business with the government on such a regular basis and who have a role in some government actions such as distribution and collection of information – I am thinking about the Information Centers, particularly – that they, too, are assigned a DoDAAD number. But they are for identification purposes only. We use them in connection with the DD 254. We use them in connection with the Personnel Security Questionnaires (PSQs). When you fill out a PSQ, at the top of it you put your FSC number. It's used in connection with our computer operations. If you'll look at the mailing label on your Industral Security Manual and Industrial Security Letters, you will find your FSC number. It's identified on the mailing labels.

Question: As things stand now, we have to find out the information from our subcontractor each time; is that right?

MR. GREEN: You ask the subcontractor and he will know what his own FSC number is.

Question: He will?

MR. GREEN: You see how simple this all is?

Jack: If all of you don't mind, we would prefer not to discuss the code numbers further. It does not relate to this problem series and you have much to do; we'll tell you. You have been issued another piece of paper. As a matter of fact, it happens to be in four parts. Jim, what are we going to do with that?

Jim: You have here part of the DD Form 254. You have the narrative guidance which is page 3. You have, if you will turn over to page 4, the beginning of blanks that you will need to complete.

Jack: We begin on page three, really.

Jim: That's right. It starts where it says "Classification Guidance." Read carefully please the paragraph that follows that, which ends with the four words, *from that base date*. Then, there is a blank that starts and continues on the next page. Your problem here is that you are now going to prepare a Prime Contractor DD Form 254.

Jack: They are now the Systems or Material Command, as you suggested. And we promised that we'd have at least a few words on what the devil the Systems Command gets with these two blasted double X papers, as a function of creating the document. Isn't that right?

Jim: Right.

Jack: We have eliminated source selections because too many steps are involved and because we want to concentrate on what you must then give as guidance – you and the Systems' Command – to your Prime Contractors.

We've asked Carolyn Meadows, member of the NCMS Board, who is in Naval Air Systems Command Headquarters, to say a few words about some of the elements that they are involved in. They will differ in each case. Carolyn does get this information (not these pieces of paper, of course). On the basis of the information described and required for your practical exercise she will tell us about just a few of the "Good God, Maude, what do I do now?" things.

Ms CAROLYN V. MEADOWS: Thank you, Jack and Jim. We receive classification guidance from the Office of the Chief of Naval Operations from, more particularly, Frank Larsen's shop. It's a part of the Operational Requirement or OR. This guide is coordinated with the cognizant technical personnel in the Naval Air Systems Command. And, in turn, a DD 254 is prepared and becomes a part of the Procurement Request that results finally in a contract.

The procurement package is brought to us for review of the classification of the Procurement Request. Each item on the DD 254 or classification guide is discussed with the technical personnel. It is compared for accuracy against the guide in the Operational Requirement. If there are any questions on the guide in the OR, CNO is contacted for clarification.

The OR provides overall systems guidance. In the case of an aircraft system, for example, the guide in the OR may say *Performance characteristics are secret*. We must determine with the help of the technical personnel which parts of the avionics equipment would reveal performance characteristics of the overall system that would warrant a secret classification. We prepare a guide for the airplane engine and for any classified avionics that are installed on the aircraft. The downgrading markings are based on those in the OR, which is a classification authority.

After the Procurement Request is reviewed and marked for classification, the contractor facility clearance research capability is verified. The DD 254 and/or classification guide is signed by me as Contracting Officer for Security Matters. It, in turn, is forwarded to the Contracts Division for execution as part of the contract package.

Jack: Thank you Carolyn. Our member of the Board from Army is Bob English, but he's in the process of moving to this area and buying a home. Regrettably he could not be with us to comment on the specific differences or similarities from Army's point of view in this process. In his place, however, Bill Horridge from the Picatinny Arsenal perhaps may be able to say a few words about how the Army procedures either differ or are the same.

Mr. WILLIAM P. HORRIDGE: From what Carolyn said, it's basically about the same thing. In fact, the question is sort of timely. Just this past week, the Chief of Staff of our new command, which is the Army Armament Research and Development Command, called us in to ask a question: how do we know when to classify? The Army being what it is, he didn't give me time to answer. He said, "put out a paper." So this is what we're doing now.

Briefly, the way we do it is, I think, much the same as the Air Force and the Navy does it. To me the two questions are when and how to classify. Generally, our command gets a request to come up with a new system either to modify an existing system or to come up with, for example, a system that will shoot bullets at right angles - or some similarly new capability or concept.

So, what we do as a component, is to try to make an initial determination of the classification. This determination will be a combined decision coming out of a meeting with many specialists. For instance, there will be a security specialist. I guess that you would consider that we are experts in classification management; an engineer probably from the project office or the project manager's office, as the case may be; the foreign intelligence people, from whom we get a lot of information; probably also, as Mr. Larsen commented, the counterintelligence people — we do have a small detachment of counterintelligence people on-base.

After these decisions are made as to what the classification will be, we then prepare a detailed guide which we send up to the Department of Army for their approval.

Comment from audience: Not any more. You no longer send a guide to DA for approval.

MR. HORRIDGE: You're right. I stand corrected.

Question: Do you in the Army assign any data technique process at all?

MR. HORRIDGE: No, we don't. I know that they're not assigned *per se*. They may get into the process. The project manager or the project officer is responsible for the whole ball of wax but he doesn't get into making the decision.

Jack: So, now you have some further quiet time. We are going to, from here on out, work as groups. The reason is that we expect there will be representation among you on one or another facet of each of these things that we will encounter. So for this purpose, the tables will be divided. We recommend that you work together on the points which should be considered, developed and provided. Your first requirement is to create the missing information for the *unclassified* narrative guide. That is directed to only one of two subsystems. You'll note on the front page of the DD 254 where it describes what is being bought, that it describes a target acquisition and designation system *and required communications*. I apologize that I didn't have quite enough space to spell out the word.

So, now you are the Systems or Material Command. You have the Operational Requirement, if you are Navy, or you have the Scientific and Technical Objective, if you are Army. They are much one and the same. With the views of Headquarters without reflecting the determination on downgrading and declassification and the requirements documents — that was, of course, intentional. You have to read the other words contained to come to a conclusion. So Mr. Systems Command, what do you say to the Prime Contractor without a DD 254c?

Jim: Please consult with each other.

Jack: Adjust your chairs so you can chat.

Work Time

Jim: The next step in the exercise, now that you have "completed" your role as Systems Command (or Material Command) is for you to become the Prime Contractor. Remember, from our earlier comments, that the preliminary steps of the Contracting Agency such as the RFP and the RFQ have been excluded for the purpose of this exercise. Obviously, these are important in the procurement and guidance processes — for example, the DD Form 254 which is issued with the Request for Proposal to a number of prospective contractors must be interpreted and/or modified as questions arise. Frequently, the 254 issued with a contract has been changed markedly from that issued with the proprosal. As I said, these steps have been eliminated from this exercise because of time considerations as well as for simplifying considerations. We have had the explanations of Frank Larsen

as a Headquarters representative and Carolyn Meadows and Bill Horridge as Systems/Material Command representatives. Now, to explain further the role of the Prime Contractor, we will hear from Jim Buckland, Martin-Marietta Corporation – incoming President of NCMS – Dean Richardson, Texas Instruments – outgoing President of NCMS – and Dick Butala, Hughes Aircraft Corporation – incoming and outgoing Vice President of NCMS. All have similar approaches and needs as one views this topical area, so Jim, with consultation, will make the presentation.

Mr. JAMES A. BUCKLAND: When we in Martin-Marietta receive a DD 254 with a Request for Proposal (RFP), we dissect it to determine: what will be its effect on the company in contract performance? Obviously, we check to learn if the guidance is adequate. and if not, to see further guidance and information from the Contracting Agency. In this connection, the type of contract to be awarded is important – is it to be Cost Plus Fixed Fee?Cost Plus Incentive Fee? Fixed Price? Each type of contract brings its own set of problems which must be considered and analyzed. It is here that the specificity of the DD 254 becomes important. As we all know, security is costly. Classified contracts cost more than unclassified. Does the guidance give the company sufficient information in order for decisions to be made which will identify those components, sub-systems and systems that can be manufactured in open areas and under unclassified conditions with uncleared people? Will it be possible to establish a fixed point at which the unclassified parts may be brought together and classified?What are the documentation requirements? Will the company be required to furnish with the systems, detailed technical manuals, both classified and unclassified? Is it possible to design the system so that major parts of the documentation may be unclassified, and only final assembly manuals and associated drawings need to be classified?

How much sub-contracting will be necessary? Will we be permitted to contract for whole sub-systems from a qualified contractor which will, at a later time, be integrated into the total system and classified accordingly then? What security guidance will the sub-contractor need, if any? Will it be possible to contract for unclassified systems, which will ease the guidance problem? If unclassified procurement is possible, will there be other problems such as: to what extent will there be a requirement for limiting future sales by the sub-contractor? Is the system or parts of it subject to the Export Control Statutes and Regulations? Will Export Licences be required? Is the system or parts thereof subject to the International Traffic in Arms Regulation (ITAR)?

Will the prime or sub-contract involve the inclusion of Proprietary Data which, under the Armed Services Procurement Regulations (ASPR), must be specifically identified and marked? I might add that failure to mark is our loss, even though the ASPR provides a limited time to rectify any mistakes.

All these and many other facets of the contract are studied throughout its life starting with the RFP and through the final delivery and final payment. Don't forget, if the contract is subject to renegotiation at any stage of performance, guidance, or lack of guidance, plays a major role.

Finally, we prepare and issue sub-contractor DD 254s and are prepared to run interference for the sub-contractor when necessary, as well as providing further guidance. We make the sub-contractor aware of changes in User Agency requirements during the life of the contract until completion and final payment.

Your task as the Prime Contractor is to consider all of these variables and to present to your company and the User Agency the best options possible. You have all heard of the balance between the "Right to Know" and the "Need to Know." In contracting, there is another balance to be maintained – to protect the information required to be protected at the lowest possible cost (*i.e.*, classification level) to permit your company to make a profit, while, at the same time, facilitating its ability to sell the product without interference; truly a balancing act! A key point is to define the security problem as narrowly as possible so that the balance may be preserved. Consequently, the guidance provided by the User Agency must be precise and the contractor interpretation reasonable. It is in that frame of reference that you need to decide what information you must provide to your chosen sub-contractor Wizard Electronics. Remember that even as Jim said earlier with respect to eliminating the RFP, RFQ phases from the determination of the Prime Contractor effort, so too is it essentially eliminated from this stage; we are dealing with only one potential sub-contractor.

Work Time

Jim: The final phase, as you might imagine, is that you are now the sub-contractor responding to a request for a proposal on the communications subsystem from the Prime Contractor and having been provided with the agreed guidance. Your final actions require you to determine, based on all you have done so far, the classification and markings to be applied to the memorandum from the Senior Communications Engineer to the President of Wizard Electronics Corporation, describing a proposed technical approach to the problem. Jack and I are available for questions, of course, but more importantly so are Jim, Dean and Dick. Have fun!

CLASSIFICATION MARKS ARE FOR EXERCISE PURPOSES ONLY

CAPABILITY CATEGORY NO: 78-X

TITLE: COMMAND SYSTEMS

Strategic Communications	**Computer Applications**
Tactical Coummunications	**Communication Security**

I. (U) Scope: This category includes all communication systems, emphasizing the interrelationship between tactical and strategic, and the capability to exercise command over deployed forces from a variety of command levels.

2. (C) Background:

a. Initial experience gained with the deployment of the M-1 tank in Europe has confirmed that the communication capability for command and control is inadequate.

b. The present family of equipments remain vulnerable to enemy intercept and to interference. Further, they are too subject to failure as well as vulnerable to nuclear effects (especially EMP).

c.To manage control over limited forces requires significantly improved interoperability among ground units, air-to-ground units, and air-to-air units.

d. See Note below

3. (C) Concept: U.S. Forces will be generally outnumbered in tank warfare. To make the best use of limited resources requires significant advances in communications and other capabilities (see CAPABILITY CATEGORY NO: 78-XX). Secure communications between command and supporting units, including high command, is essential. The effects of such act as a force-multiplier in utilizing advances now possible in communications technology applications to achieve secure communications with and between all vehicles and command and support units. Such communications must also minimize compromise of the system even if subject to capture or other loss. Satellite-supported communications may permit essentially independent employment of our limited assets, and the possibility of extending control to higher echelons of command in emergent situations.

4. (S) Desired Capabilities

a. LPI system — maximum for a 50% probability of intercept in tactical mode circuits should not exceed 5 km range. Minimum effective range for ground wave operation to be 45 km. Secure voice capability that is capable of switching from clear to secure voice by means of a flip-flop system (this should include the inside/outside tank communication system).

b. Incorporate the most advanced anti-jam characteristics and include radiation suppression devices to ensure transmission in a high EMP environment.

c. Be capable of electronic destruct within 30 seconds of initiation. The electronic destruct circuitry shall be independent of the operating circuitry and have a separate GO-NO GO test capability. It shall be so designed to ensure against inadvertent or non-deliberate destruct (i.e., idiot proof).

5. (U) Prioritized S&T Objectives (STOs) 78-X:

The sequence of desired capabilities presented in paragraph 4 is prioritized

NOTE: Paragraphs 6-8 are not included for this application nor further background. Downgrading and Declassification must be determined

CLASSIFICATION MARKS ARE FOR EXERCISE PURPOSES ONLY

CAPABILITY CATEGORY NO: 78-XX

TITLE: CLOSE COMBAT

Tank Combat Aviation
Anti-Tank Heavy Weapons
Mechanized Infantry Light Weapons

2. (C) Background

Initial deployment of the M-1 tank in Western Europe reveals a limitation on full systems effectiveness relating to Target Acquisition and Designation. Operating at a numerical disadvantage causes a very high premium to be placed on a very high probability of first-round hit under essentially all weather conditions.

b. Intelligence predictions continue to emphasize large scale deployment (essentially complete) of the T-72 tank to Pact nations. Further, a newer, faster tank has been identified as undergoing test and expected to be deployable by 1996. It can be expected that our numerical disadvantage will continue and that the deployment of an advance tank threat will make our capability for first-round hit even more critical.

3. (C) Concept: The combined arms approach remains a mainstay of our potential to blunt an enemy thrust. In order to achieve a high probability to do this requires developing more advanced capabilities based on evolving technology in both communications and in threat-reactive, computer-assisted recognition and designation equipments. These must be compatible with the M-1 tank and Allied developments for the time period covered.

4. (C) Desired Capabilities:

a. All weather operation, including operations in self-generated smoke, dust and fog.
b. Minimum of 6 km range to be achieved in suitable terrain.
c. Accuracy necessary to acquire and designate a target 30mm in size at the minimum range (NOTE: The term designate shall be interpreted to mean the capability of the Target Acquisition and Designation system to penetrate camouflage; for example, the muzzle of the gun of a camouflaged tank).
d. System must operate independently of the fire control system.
e. Size limits – May not exceed 1 cubic foot in overall size, nor 30 pounds in total weight (including power supply).
f. Shall be mounted co-axially with the main gun tube.
g. Must be full unit replaceable/module replaceable by tank crew. Unit/module must have GO-NO GO test and operation capability.
h. System power supply must be capable of 6-hours of independent operation and must be capable of operating with main power supply of the vehicle.

5. (U) Prioritized S&T Objectives (STOs) 78-XX:

The sequence of desired capabilities presented in paragraph 4 is prioritized.

NOTE: Paragraphs 6-8 are not included for this application.

Downgrading and Declassification must be determined

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

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED 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)*		
X	a. PRIME CONTRACT	a. PRIME AHC-1234-82-0000	30Sep1985	X	a. ORIGINAL (complete in all cases)	Date 10May1982
	b. SUBCONTRACT *(Use Item 8 to identify further subcontracting)*	b. FIRST TIER SUBCONTRACT			b. REVISION NO. *(Supersedes all previous specifications)*	Date
	c. INVITATION TO BID OR REQUEST FOR PROPOSAL	c. INVITATION FOR BID, REQUEST FOR PROPOSAL, or request for quotation.	Due Date		c. FINAL	Date

5a. Is this a follow on/related contract? ☐ Yes ☒ No. If Yes, give preceding contract No. and date preceding contract was completed:
b. Accountability for classified material on preceding contract may be transferred to this follow-on/related contact (Complete only if item 5a. has "Yes" answer) ☐ Yes ☐ No.

6a. Name, Address (include Zip Code) and FSC Number of Prime Contractor. *	b. Name and Address (include Zip Code) of Cognizant Security Office.
XYZ High Technology Corporation 1111 L.S.I Boulevard Anywhere, U.S.A. 99999 FSC A33333	DCASR PODUNK 10-4 Way Out Street Euphoria, PT 00001
7a.* Name Address (include Zip Code) and FSC Number of first tier subcontractor.	b. Name and address (include Zip Code) of Cognizant Security Office.
8a. *Name, Address (include Zip Code), and FSC Number of Second Tier Subcontractor, or facility associated with IFB, RFP, or RFQ.	b. Name and address (include Zip Code) of Cognizant Security Office.

*When actual performance is at a location other than that specified, identify such other location in Item 13. Not Applicable

9a. General identification of the Procurement for which this specification applies. Target Acquisition & Designation System & Required Comm.
b. DoDAAD Number of Procuring Activity identified in Item 14a. DAHC00
c. Are there additional security requirements established in accordance with paragraph 1-113 or 1-115, ISR? ☐ Yes ☒ No. If Yes, identify the pertinent contractual documents in Item 13.
d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? ☐ Yes ☒ No. If Yes, explain in Item 13 and identify specific areas or elements.

10. ACCESS REQUIREMENTS	Yes	No	ACCESS REQUIREMENTS	Yes	No
a. Access to Classified Material Only at other contractor/Government activities.		X	j. Access to SENSITIVE COMPARTMENTED INFORMATION.		X
b. Receipt of classified documents or other material for reference only (no generation).		X	k. Access to other Special Access Program Information (specify in Item 13).		X
c. Receipt and generation of classified documents or other material.	X		l. Access to U.S. classified information outside the U.S., Panama Canal Zone, Puerto Rico, U.S. Possessions and Trust Territories.		X
d. Fabrication/Modification/Storage of classified hardware.	X		m. Defense Documentation Center or Defense Information Analysis Center Services may be requested.	X	
e. Graphic arts services only.		X	n. Classified ADP processing will be involved	X	
f. Access to IPO information.	X		REMARKS:		
g. Access to RESTRICTED DATA.	X				
h. Access to classified COMSEC information.	X				
i. Cryptographic Access Authorization required.	X				

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. The classification guidance contained in this specification and attachments referenced herein are complete and adequate.	b. Activity address (Include Zip Code), Telephone number and office symbol.
Chip Vinel Chip Vinel, M-1 Tank Project Manager Signature, Typed name and title of program/project manager (or other designated official)	U.S. Army Immaterial Command (IMMAT-1) Off Beat Station Alexandra, VA 22XXX (703) 007-0000

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 (provisional) THIS FORM REPRESENTS THAT APPROVED AT OASD (SP) AND READY FOR ISSUE SUBJECT TO THE NOTE CONTAINED IN ITEM 12

12. This concerns public release of information pertaining to classified contracts and (as of 22 April 1977) has not been fully coordinated within the Office of the Secretary of Defense.

13. Security Classification Specifications for this solicitation/contract are identified below (check applicable item and supply attachments as required). Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 13b. The following information must be provided for each item of classified information identified in an extract or guide:
(i) category of classification,
(ii) schedule for downgrading/declassification (ADS, GDS, or XGDS),
(iii) declassification date, and
(iv) where exemption (XGDS) has been authorized the exemption category(ies) shall be identified, the authorizing official shall be identified by title or position, or applicable classification guide(s) shall be cited.
The official named in Item 11a. is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification.

[X] a. A completed narrative is (1) [X] attached, or (2) [ ] transmitted under separate cover and made a part of this specification.

[X] b. The following classification guide(s) is made a part of this specification and is (1) [ ] attached, or (2) [X] transmitted under separate cover. (List guides below or in an attachment by title, reference number and date).

[ ] c. Service-type contract/subcontract. (Specify instructions in accordance with ISR/ISM, as appropriate.)

[ ] d. In response to the contractor's request dated _____, retention of the identified classified material is authorized for a period of _____. (NOTE: Do not complete if Items 5a. and b., have "Yes" answer; to be completed only for a Final DD Form 254.)

[ ] e. Annual review of this DD Form 254 is required. If checked, provide date such review is due: _____

[X] f. Remarks. (Whenever possible, illustrate properly worded downgrading/declassification stamp.)

Access to Foreign Intelligence information relating to armor and communications threats is required and authorized.

The original TS Classifying Authority for items of information shown on the guidance providedto be exempted from the general declassification schedule of EO 11652 is the Commanding General, U.S. Army Immateriel Command – unless otherwise designated on the guidance in question.

Transmitted under separate cover is Security Guidance – Improved Communications Sub-system, M-1 Tank, dated 01May1982, Secret, XGDS-3, Declassified 31Dec2007, hereby made a part of this specification.

Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Official named in item 14b. below, or by the Prime Contractor, as authorized.

REQUIRED DISTRIBUTION:

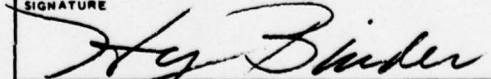
[X] PRIME CONTRACTOR *(Item 6a)*
[X] COGNIZANT SECURITY OFFICE *(Item 6b)*
[X] ADMINISTRATIVE CONTRACTING OFFICE *(Item 14b)*
[X] Quality Assurance Representative
[ ] SUBCONTRACTOR *(Item 7a)*
[ ] COGNIZANT SECURITY OFFICE *(Item 7b)*
[X] Program/Project Manager (Item 11a.)
[X] U.S. Activity Responsible for Overseas Security Administration

ADDITIONAL DISTRIBUTION:

[ ]
[ ]

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

Hy Binder, Contracting Officer

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

U.S. Army Immateriel Command (Immat-C)
Off Beat Station
Alexandra, VA 22XXXX

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

John Watt, Administrative Contracting Officer
Government Representative, XYZ High Technology Corporation
1111 L.S.I. Boulevard
Anywhere, USA 99999

ATTACHMENT TO DD FORM 254, DATED 10 MAY 1982
XYZ High Technology Corporation

NARRATIVE GUIDANCE AND SYSTEMS REQUIREMENTS

1.*Background* —Technology advances permit examining means to overcome a principal element of weakness in tank warfare — the ability to acquire and recognize a target in a variety of tactical situations, and a high-order *first-round hit probability*. Further, continuing scarcity of forces makes improved communications essential. It is technologically feasible to build communications systems that minimize detectability, and are interoperable with a variety of other systems. Such improvements, if technically demonstrable, could permit command and control to be exercised from levels higher than now possible thereby improving the overall effectiveness of a limited force. The communications capability, because it is intended for tactical deployment, should minimize the effects of compromise through capture.

2.*System Goals* —

a. Target acquisition and designation sub-system

The following assumptions are related to this procurement:

- Existing tank weapons are efficient and reliable in range and probability of kill and the variety is suitable for use in a broad spectrum of missions.

- Missions will range from a one-on-one engagement in a reconnaissance-type opration to a major tank-heavy offense or defense.

Advances in the field of micro-miniaturization and packaging lead to confidence that major improvements in operations are achievable. These should include substantial improvement in the optical system and the thermal imaging system. It should include also a computer-assisted target recognition system (not including an improved IFF system that will be the subject of a follow-on development).

The target designation and acquisition system must operate independently of the fire control system and should emphasize reduced size and weight. It must include either full unit replacement or module replacement by the crew. Each sub-unit or systems must include a GO-NO GO test capability. An independent power supply, capable of operating with the main vehicle power supply, must be provided for a minimum of 6 hours of independent operation. All systems elements individually and collectively must meet the temperature, environmental and shock and vibration requirmenents of MILSPECS and MILSTANS for armored vehicles. Classified specific goals are contained in separate correspondence.

Classification Guidance

Technology supports the conclusion that the advances desired are achievable. However, technical feasbility has not been demonstrated at this time. Consequently, the General Declassification Schedule of EO 11652 is not applicable to most items of information until after the systems are in the hands of troops since the potential advantage to be gained would be lost through premature disclosure. The expected deployment date of operation capabilities for this system is expected to be 1992. The dates shown below are calculated to downgrade/declassify items of information in the concept of the General Declassification Schedule or Exempt them from the General Declassification Schedule **FROM THAT BASE DATE.**

b. Improved communications sub-system

Further information and guidance on this sub-system is provided separately as noted in Item 13.

Potential Solutions to Guidance

Target Acquisition and Designation SubSystem

1. Target Acquisition Capabilities:	
In Target Size	CXGDS-3(1998)
In Range	CXGDS-3(1998)
2. Design Details of the integrating device	SXGDS-3(2007)
Methods by which the integrating device achieves the goals	SXGDS-3(2007)*
3. Target Identification expressed in probability terms	CXGDS-3(1998)
a. Use of mini-computer	U
b. Capacity of the computer in digits	U
c. Memory capacity of computer in target types or numbers	CXGDS-3(2007)*
d. Target correlation capability (comparison between target aquired and memory capability using the sensor integrator).	SXGDS-3(2007)
4. Ability to operate in varying environments including self-induced	CXGDS-3(1998)
5. System capability on the move	CXGDS-3(1998)
6. Vulnerability of the system to RF interference expressed in probabilities of mission success in increments of ERP	SXGDS-3(2007)
7. First Round Hit Probability	CXGDS-3(1998)

*Technology to support achieving these goals may include proprietary manufacturing or design information

CLASSIFICATION MARKINGS ARE FOR EXERCISE PURPOSES ONLY

HEADQUARTERS
ARMY IMMATERIEL COMMAND
Off Beat Station
Alexandra, USA 99999

1 May 1982

Security Guidance for Improved Communications SubSystem – M-1 Tank

1. (C) *Background*

a. (C) Advances in technology lead to the conclusion that it is now practical to overcome one of the principal weaknesses of tank warfare – the ability to acquire and recognize a target in a variety of tactical situations, under all weather conditions, and to achieve a first-round on target probability in excess of 0.9. Further, it is now feasible to build communications systems which have limits on detectability, are secure and are interoperable with a variety of other systems so that command and control may be exercised from levels higher than previously possible.

b. (S) Advances in destruct technology make it possible to design systems and components which do not require physical or pyrotechnic destruct, but may be destroyed electronically. Historically, the doctrine has been physical destruct by a variety of inefficient and dangerous methods, with generally unsatisfactory results. The motive was to prevent an enemy from gaining an insight into design criteria and logic. Equipment in the field generally is not state-of-the-art. Similarly, advances in coding technology make it possible to use single, one-time coding systems which, even though captured or compromised in a tactical situation do not compromise the overall system. However, the concept presented herein is revolutionary, rather than evoluntianary, hence, of itself requires protection.

2. (S)*Classification Guidance*

NOTE: Downgrading and Declassification must be determined

3. (C)*Classification Rationale*

The categories of information being exempted are deemed to require protection for an extended period because

- Intelligence assessments indicate no evidence to support development along these lines by potential adversaries;
- Lead-time for development is viewed as long-term since the technical feasibility has not been demonstrated; and
- A significant advantage will accrue and be retained even when deployment begins, until or unless active hostilities cause the loss of one or more systems despite the destruct mechanisms.

Item will be downgraded to Confidential on deployment to operational commands. Items will not be declassified in accordance with existing law, unless compromises of the type described above occur; such will be a matter of specific separate advice.

Items will be declassified 15 years after deployment to operational commands or in 2007 whichever is later (and subject to earlier specific declassification action dependent upon other events).

J. G. LAW
General, U.S. Army

CLASSIFICATION MARKS ARE FOR EXERCISE PURPOSES ONLY

Potential Solution to Paragraph 2 of Hq. AIC Security Guidance
Improved Communications Sub-system – M-1 Tank

a. (C) The fact that a secure communications system is being developed for tank installation		C-1998
b. (U) The fact that a new communications system is being developed for tank installations		U
c. (U) The degrees of interoperability with other communications systems		U
d. (C) The fact that electronic destruct will be utilized in the system		S-2002
e. (C) Design details (may be proprietary)		
(1) Details of non-comsec portion of the system		C-1997
(2) Design details of the comsec portion		S-2007
(3) Details of the electronic destruct system		S-2002
(4) Integration plans and drawings which reveal system performance		S-2002
(5) Details of individual components and sub-systems	(may be as high)	S-2002
f. (C) The use of radiation suppression devices in the systems		C-1997
g. (C) Design details of the suppression devices	(may be as high)	S-1997
h. (C) The method of initiating electronic destruct		C-1997
i. (C) The efficiency of the radiation suppression system in DBM		S-1997
j. (U) External views of the antenna system		U
k. (U) Design details of the antenna system		C-1997
l. (U) System vulnerability to intercept		S-2007
m. (U) System vulnerability to EMP		S-2007

NOTE: The Downgrading and Declassification determination would go on the basic memorandum
This particular example has eliminated the GDS/XGDS approach in view of its probable demise

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

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED 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)*		
	a. PRIME CONTRACT	a. PRIME AHC-1234-82-0000		X	a. ORIGINAL (complete in all cases)	Date 01Jun1982
	b. SUBCONTRACT *(Use Item 6 to identify further subcontracting)*	b. FIRST TIER SUBCONTRACT			b. REVISION NO. *(Supersedes all previous specifications)*	Date
X	c. INVITATION TO BID OR REQUEST FOR PROPOSAL	c. INVITATION FOR BID, REQUEST FOR PROPOSAL, or request for quotation. RFP, XYZ High Technology Corp No.123	Due Date 01Sep1982		c. FINAL	Date

5a. Is this a follow on/related contract? ☐ Yes ☒ No. If Yes, give preceding contract No. and date preceding contract was completed:

b. Accountability for classified material on preceding contract may be transferred to this follow-on/related contact (Complete only if item 5a. has "Yes" answer) ☐ Yes ☐ No.

6a. Name, Address (include Zip Code) and FSC Number of Prime Contractor. *	b. Name and Address (include Zip Code) of Cognizant Security Office.
XYZ High Technology Corporation 1111 L.S.I Boulevard Anywhere, U.S.A. 99999 FSC A33333	DCASR PODUNK 10-4 Way Out Street Euphoria, PT 00001
7a.* Name Address (include Zip Code) and FSC Number of first tier subcontractor. Wizard Communications Corporation Ampere Street, Box 69 Rhovolt, U.S.A. 66666	b. Name and address (include Zip Code) of Cognizant Security Office. DCASR RHOVOLT 9876 Ohm Boulevard Rhovolt, U.S.A. 66666
8a. *Name, Address (include Zip Code), and FSC Number of Second Tier Subcontractor, or facility associated with IFB, RFP, or RFQ.	b. Name and address (include Zip Code) of Cognizant Security Office.

*When actual performance is at a location other than that specified, identify such other location in Item 13. Not applicable

9a. General identification of the Procurement for which this specification applies. M-1 Tank Improved Communications System
b. DoDAAD Number of Procuring Activity identified in Item 14a. DAHC00 plicable
c. Are there additional security requirements established in accordance with paragraph 1-113 or 1-115 ISR? ☐ Yes ☒ No. If Yes, identify the pertinent contractual documents in Item 13.
d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? ☐ Yes ☒ No. If Yes, explain in Item 13 and identify specific areas or elements.

10. ACCESS REQUIREMENTS	Yes	No	ACCESS REQUIREMENTS	Yes	No
a. Access to Classified Material Only at other contractor/Government activities.		X	j. Access to SENSITIVE COMPARTMENTED INFORMATION.		X
b. Receipt of classified documents or other material for reference only (no generation).		X	k. Access to other Special Access Program Information (specify in Item 13).		X
c. Receipt and generation of classified documents or other material.	X		l. Access to U.S. classified information outside the U.S., Panama Canal Zone, Puerto Rico, U.S. Possessions and Trust Territories.		X
d. Fabrication/Modification/Storage of classified hardware.	X		m. Defense Documentation Center or Defense Information Analysis Center Services may be requested.	X	
e. Graphic arts services only.		X	n. Classified ADP processing will be involved	X	
f. Access to IPO information.	X		REMARKS:		
g. Access to RESTRICTED DATA.		X			
h. Access to classified COMSEC information.	X				
i. Cryptographic Access Authorization required.	X				

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. The classification guidance contained in this specification and attachments referenced herein are complete and adequate. Chip Vinel, M-1 Tank Project Manager Chip Vinel Signature, Typed name and title of program/project manager (or other designated official)	b. Activity address (Include Zip Code), Telephone number and office symbol. U.S. Army Immaterial Command (IMMAT-1) Off Beat Station Alexandra, VA 22XXX (703) 007-0000

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 (provisional) THIS FORM REPRESENTS THAT APPROVED AT OASD (SP) AND READY FOR ISSUE SUBJECT TO THE NOTE CONTAINED IN ITEM 12

12. This concerns public release of information pertaining to classified contracts and (as of 22 April 1977) has not been fully coordinated within the Office of the Secretary of Defense.

13. *Security Classification Specifications for this solicitation/contract are identified below* (check applicable item and supply attachments as required). Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 13b. The following information must be provided for each item of classified information identified in an extract or guide:
(i) category of classification,
(ii) schedule for downgrading/declassification (ADS, GDS, or XGDS),
(iii) declassification date, and
(iv) *where exemption (XGDS) has been authorized the exemption category(ies) shall be identified, the authorizing official shall be identified by title or position, or applicable classification guide(s) shall be cited.*
The official named in Item 11a. is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification.

- [x] a. A completed narrative is (1) [x] attached, or (2) [ ] transmitted under separate cover and made a part of this specification.
- [ ] b. The following classification guide(s) is made a part of this specification and is (1) [ ] attached, or (2) [ ] transmitted under separate cover. (List guides below or in an attachment by title, reference number and date).
- [ ] c. Service-type contract/subcontract. (Specify instructions in accordance with ISR/ISM, as appropriate.)
- [ ] d. In response to the contractor's request dated _____, retention of the identified classified material is authorized for a period of _____. (NOTE: Do not complete if Items 5a. and b., have "Yes" answer; to be completed only for a Final DD Form 254.)
- [ ] e. Annual review of this DD Form 254 is required. If checked, provide date such review is due: _____
- [x] f. Remarks. (Whenever possible, illustrate properly worded downgrading/declassification stamp.)

Access to Foreign Intelligence information relating to communications threats is required and authorized.
The original TS Classifying Authority for items of information shown on the guidance required to be exempted from the general declassification schedule of EO 11652 is the Commanding General, US Army Immateriel Command – unless otherwise designated on the guidance in question.

Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Official named in item 14b. below, or by the Prime Contractor, as authorized.

REQUIRED DISTRIBUTION:

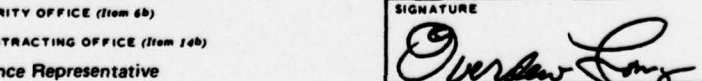
- [x] PRIME CONTRACTOR *(Item 6a)*
- [ ] COGNIZANT SECURITY OFFICE *(Item 6b)*
- [x] ADMINISTRATIVE CONTRACTING OFFICE *(Item 14b)*
  - [x] *Quality Assurance Representative*
- [x] SUBCONTRACTOR *(Item 7a)*
  - [x] COGNIZANT SECURITY OFFICE *(Item 7b)*
- [x] Program/Project Manager (Item 11a.)
- [ ] U.S. Activity Responsible for Overseas Security Administration

ADDITIONAL DISTRIBUTION:

- [ ]
- [ ]

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

Overdew Long, Contracting Officer

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

U.S. Army Immateriel Command (IMMAT-4)
Off Beat Station
Alexandra, VA 22XXX

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

John Watt, Administrative Contracting Officer
Government Representative, XYZ High Technology Corp.
1111 L.S.I. Boulevard
Anywhere, U.S.A. 99999

WIZARD COMMUNICATIONS CORPORATION
Ampere Street, Box 69
Rhovolt, U.S.A. 66666

1 August 1982

MEMORANDUM TO PRESIDENT

From: Senior Communications Engineer

Subj: Request for Proposal No. 123, XYZ High Technology Corporation

1. ( ) Subject request establishes requirements for operation not now achievable. However, the state of the art in solid state devices (from the point of view of modest cost because of our proprietary production techniques – of combining several discrete functions into one device) there is a technologically feasible approach. Some advances in marrying discrete functions need to be made.

2. ( ) The established requirement that there be a "flip-flop" system for secure transmission or plain text transmission is quite new. Heretofore packaging alone would have made such an approach infeasible from the point of view of size and weight alone. Our recently developed combining of functions – one we haven't actually used – is particularly applicable and can make a significant difference. I recommend that it be outlined for the propposal. It will meet the requirement of field (i.e., crew) replacement and test.

3. ( ) The encoding requirements with our latest chip technology can be accomplished by a communications support facility at the Division or Corps. We are at the one-time-use code status, with this advance, that has not been employed previously. The simplicity of the design will permit changing codes within a minute or two, as you may remember from our paper No. 007-82 of June this year.

4. ( ) An additional requirement posed is that there be an electronic destruct capability. As established in our paper 007-82, the logic is such that when the voltage described is applied no possibility exists that any techniques (known or proposed) will recover the code. Hence, the objective is served that the device can be discarded as trash when decoded.

5. ( ) The packaging techniques we can use will ensure that the device cannot be disassembled without its breaking. A residual piece could not reveal useful information. Non-destruct methods of examination (such as X-ray, infrared, laser, ultra-sonic) would not reveal the design techniques.

6 ( ) The above is a summary of the most salient new elements involved in the request. It would appear to me that we can manage to produce a truly important advance in the state of the art based upon our own independent R&D program.

STEINMETZER

Answer: 1.(U);2.(C); 3.(S); 4.(S); 5.(C);6.(U). Declassified 2002.

CLASSIFICATION MARKINGS ARE FOR EXERCISE PURPOSES ONLY