CLASSIFICATION MANAGEMENT

JOURNAL OF THE NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME IX - 1973

Typography

Decarol S. Pyles

Published semiannually. Annual subscription, $10.00. Mailing address: Executive Secretary, National Classification Management Society, P.O. Box 7453, Alexandria, Virginia 22307 Lorimer F. McConnell and Jack Robinson, Editors. Views expressed by individuals herein do not necessarily represent views of their employers or of the National Classification Management Society.

NATIONAL CLASSIFICATION MANAGEMENT SOCIETY

PAPERS FROM THE NINTH NATIONAL SEMINAR
(July 17–19, 1973)

CONTENTS

Report of the President – NCMS Looks Ahead . . . . . *iii*
Mr. James J. Bagley, President
National Classification Management Society

Secrecy and the Right to Know *1*
Dr. James B. Rhoads

Discussion of Section XI–National Security–
Proposed Federal Criminal Code *3*
Mr. Walter G. Fenerty
Mr. Robert L. Keuch
Mr. Robert C. Maynard

The Pentagon Papers–Who Won? *14*
Mr. Sanford Ungar

Computers and Automated Classification–1980 . . . . . *19*
Dr. Lawrence G. Roberts

Insight into the Bell System Plans for 1980 and Beyond *29*
Mr. Charles P. Buckley

Progress and Effects of Implementation of Executive Order
11652 and Projections for the Future *32*
Mr. Jack Robinson
Captain Richard E. Myers, USA
Mr. Daniel J. Dinan
Mr. Lawrence C. Myers
Mr. Arthur F. Van Cook

New Industrial Security Policies *44*
Colonel Donald T. Clark, USA

Our Credibility Gap is Showing *53*
Mr. Dean Richardson

Congress Looks at E.O. 11652 . . . . . *56*
Mr. William G. Phillips
Mr. Al Friendly, Jr.
Dr. Earl Callen

Secrecy Agreements and Statements Involving Classified Information *66*
Mr. William G. Florence

Classification and Foreign Military Sales *70*
Mr. Edward Silver
Mr. C. C. Fredericks
Mr. Leonard A. Alne

Classification and the Smaller Research Groups *86*
Mr. John D. Kettelle

REPORT OF THE PRESIDENT

NCMS LOOKS AHEAD

Mr. James J. Bagley
National Classification Management Society
President, 1972-1973

In the nearly ten years of its existence NCMS has been in the forefront of action to bring order out of the classification chaos that has existed throughout Government and industry. The NCMS seminars and publications have been the source of much of the information that exists in the field of classification management.

The Past

It is useful to recall some of the past seminars and to highlight a few of the many noteworthy events. The Honorable John E. Moss, keynote speaker at the Third Seminar in 1967, detailed the background of the Freedom of Information Act (5USC522), which became effective on July 4, 1967. In his remarks he reminded the attendees of their responsibilities regarding the classification of information, saying:

> "You handled it. You saw the nature of the content, the degree of sensitivity, the impact of that which is not available. You have a very serious responsibility each time you make a judgment, advocate a policy, or determine a classification, because at each point you have determined that a small portion of the totality of information is not going to be available finally to those who have the greatest need for it. I hope that it's always a balanced judgment.
>
> "In a society where each and every one of us is a part of Government, it is essential that each and every one of us has an absolute maximum of information available in making the very important decisions we must make as our own governors."

Congressman Moss' comments are particularly appropriate now when one looks at the searching reviews of the Freedom of Information Act made by the Congress.

At the Fifth Seminar, in 1969, a preliminary report was made by a Special Task Group on the Dissemination of Information, established by the Committee on Scientific and Technical Information of the Federal Council on Science and Technology. The Task Group was charged with reviewing the policies and practices of the federal agencies on the dissemination of information in the light of the Freedom of Information Act and with making recommendations on steps that might be taken to improve dissemination.

The Seventh Seminar, in 1971, saw NCMS embroiled in the Pentagon Papers controversy, which produced some unfortunate and unfair publicity. Little did the attendees think at that time that the papers would be the tip of what would later become Watergate.

E.O. 11652 was the primary subject of discussion, at the Eighth Seminar in 1972; the first comprehensive discussion of the Order with details on implementation.

The Present

While it is always useful to look at the past, it is only useful when the past can be the prelude to the present and the precursor of the future. NCMS has historically taken the position that it should cooperate with other societies that have similar goals. Also, to make its positions known to Congress, as well as agencies of the Government, NCMS has established a liaison with several committees of the House and Senate and has furnished to these committees pertinent NCMS reports, studies and positions. Society representatives have presented testimony on bills under discussion.

To date NCMS has presented its comments on the merits of proposed bills and has made clear that the position was based on its independent judgment of the merits of a bill and not an echo or reiterated comments of other groups. The society has striven to maintain its independent position in all matters and has not allowed its position to be compromised by matters not strictly related to classification principles and practices.

The following are some of the actions taken.

NCMS has established liaison with the Civil Service Commission and has furnished information on the aims and scope of the Society, our literature and bulletins. It is our hope that this will lead to the development of standards for classification management personnel.

Over the last 18 months there has been direct communication with the Department of Defense on a variety of matters. To cite a few of the NCMS recommendations supported by study of the issues,

- To establish a classification management function in all Government and defense agencies dealing with classification matters.
- To revise the authorizations and determinations regarding contractors retaining documentary materials.
- To continue automatic downgrading information established as Group 3 under E.O. 10501 rather than making it "Excluded" under E.O. 11652. (We are pleased to note concurrence of DoD reported subsequently in these proceedings.)
- To eliminate or at least restrict approval for Special Access Programs.

This is where we are today. We know that classification is here to stay and that it is more important now than at any time in the past. E.O. 11652 has established a new baseline for an improvement in the system.

The results of a survey on classification conducted in 1971 was distributed in 1972 to Congress, Government agencies, and interested societies as well as to NCMS members. It is interesting to note that many of the views of NCMS were included in the provisions of E.O. 11652. For example:

- Creation of an Inter Agency Classification Review Committee.
- Acceleration of the downgrading and declassification schedule.
- Limitation on the number of people authorized to classify.
- Identification of individuals authorized to classify.
- Redefinition of information which qualifies for classification into various categories.
- Determination, by mandatory review after a specified time, of current classification of information not subject to automatic declassification.

Early in 1972 NCMS set up contacts with the Executive Director, ICRC, and initiated in-depth conversations on implementation and enforcement problems of E.O. 11652. There is reason to believe that much of the progress made in the implementation of the Order is based on these discussions.

The NCMS Board has established liaison with the following groups:

American Society for Industrial Security
National Security Industrial Association
Council of Defense, Space, and Industrial Agencies
Aerospace Industries Association

Liaison is through Board and Society members who participate directly in these groups and not as a formal association. The reason that formal association is inappropriate is that positions of these societies are not all relevant to the NCMS goals. However, when the subject matter is one on which NCMS has concern, it takes a position.

The Future

Classification is the tap root of the information security system. Classification establishes the need for security systems to control and protect information. Personnel and physical security come into being after it has been established that information requires protection.

Although there has been a marked improvement in the classification program since 1963, many problems remain. From the publication of the Pentagon Papers in 1971 to the present (aggravated by Watergate), at least a dozen bills or resolutions have been introduced in Congress to establish new classification systems. Unfortunately, most intermingle two separate and distinct problems—classification and executive privilege. It is our contention that these subjects are separate and should not be combined. Classification is a problem to which a solution, with time, may be found. Executive privilege is a question of such profound proportions that a solution by mere mortals may never be possible.

In 1972, two revisions of the U.S. Criminal Code were introduced, one by the Senate Committee on the Judiciary, and one by the Justice Department. In part, the thrust of both bills is to better protect information that requires protection; only the approach is different. The Board has had both versions under study for sometime and will, when appropriate, present its position. In this regard, the exposition of both versions by the panelists at the Ninth Seminar was very useful.

Independent review of the effectiveness of E.O. 11652 is needed, and NCMS could make a valuable contribution. In addition to the normal policing of the order, the following areas appear to warrant particular attention:

- The tendency of agencies to blanket entire programs as exempt—rather than only those explicit items that *may* warrant such exemption.
- Habitual use of 30 years as the normal declassification date of exempted material.
- A more precise definition of Exempt-Category 3.
- An official definition of the vague term "intelligence sources and methods," and guides to aid in determining whether defined factors are present.

Society Action Opportunities

1. Of singular importance to the Society is the recognition of classification management as a profession which can best be served by the establishment of job standards. The Society Board of Directors is now drafting such standards and they will ultimately be forwarded to the Civil Service Commission for its consideration. As noted previously the Commission has already received considerable NCMS literature.

2. An NCMS position should be prepared and submitted to the appropriate subcommittees of the Congress on the proposed revision to Title 18, United States Code as it affects the control and dissemination of classified information.

3. Because its members represent a good cross section of Government and industry, NCMS is in an especially good position to assess the effectiveness of the implementation of E.O. 11652. The Society should establish methods for acquiring, interpreting and reporting its findings to the ICRC and the Government. In this regard, NCMS is in a unique position to get the "straight dope" which is not filtered or watered down by official positions.

4. The United States has many international agreements, some of which involve the transfer of information, that must be protected by the holders. Steps should be taken to include in protocols agreements relating to the downgrading and declassification of information. ■

SECRECY AND THE RIGHT TO KNOW

Dr. James B. Rhoads,
Acting Chairman of the ICRC

I am delighted at having this opportunity to speak to those who have the responsibility for managing classified documents. Events of the last several years have focused a great deal of public attention on the Government's policies and programs in this area, and have forced those of us who must deal with classified documents to make a careful re-examination of the twin issues of secrecy and disclosure. The publication of the "Pentagon Papers," the issuance of the President's new Executive Order, and more recent events have made the general public more records-conscious and more secrecy-conscious than ever before. As a result, organizations such as yours and meetings like this one, where the issues and problems can be discussed freely and openly, have taken on an importance which none of us could have foreseen a few years back. I hope that my few remarks can be a contribution to the dialogue on our common problem of secrecy and the right to know.

As you know, on March 8, 1972, President Nixon issued Executive Order 11652 establishing a new, and more progressive, system for the classification and declassification of Government documents relating to national security. The New Order sought to revise a system which had grown progressively more cumbersome and unresponsive to realistic security requirements. For all practical purposes, the classification of documents began during the First World War, grew to maturity during the Second World War, and became the standard practice of most Government agencies during the Cold War. The atmosphere of warfare, or the threat of warfare, created an institutional bias in favor of secrecy at the expense of the public's right to know. Far too many documents were classified by thousands of classifiers whose actions received only minimal review. No one knew or could even make a reasonable guess at the number of classified documents that existed throughout the Government. Citizens had no idea how to go about getting access to these records. And, perhaps the most one-sided aspect of the classification system was that while the most elaborate provisions had been made for classifying documents and protecting them, once classified, only minimal provisions had been made for declassifying them.

The issuance of Executive Order 11652 marked the culmination of over a year's effort by many individuals throughout the Government who had come together to revise the system of handling classified information. It also marked the beginning of a new era in the Government's approach to the classification system. The new Order included ideas which had been discussed by scholars and the public for many years but which had never found wide-spread acceptance within the Government. One of these ideas was the concept of the people's right to know about the way their Government operates. President Nixon endorsed this idea in the introduction to the Order by stating that "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 more than just including some nice sounding phrases about the people's right to know, provisions which could turn those ideals into reality were an essential part of the Executive Order and the implementing Directive of the National Security Council.

The Order and the Directive sought to balance more equitably the legitimate need for secrecy with the equally legitimate need for an informed public through access to the records of Government. Stated simply, the new Order established a system that would classify fewer documents, and would declassify more information sooner. To help make this system a practical reality, an Interagency Classification Review Committee was established to assist the National Security Council in monitoring the implementation of the Order and the Directive. For the first time a centralized reviewing authority was set up to check on exactly how the agencies and departments were fulfilling the promised changes in the system. The Committee members include a Chairman designated by the President, the Archivist of the United States, and senior representatives of the departments of Defense, State, and Justice, the Central Intelligence Agency, the Atomic Energy Commission, and the National Security Council Staff. As Chairman, Ambassador John Eisenhower directed the Committee's first year of operation. In April I was designated Acting Chairman of the Committee to succeed Ambassador Eisenhower. The Committee meets monthly to review agency compliance with the Order's provisions, to hear complaints about the operation of the system from both the public and Government officials, to decide matters of interpretation of the Order and Directive, and to hear appeals from the public when their requests for declassification have been denied by an agency or department.

The classification and declassification system which the Order and Directive established and which the Interagency Classification Review Committee monitors has tightened the definitions of Top Secret, Secret, and Confidential classified information. A new General Declassification Schedule was established for speedier, automatic downgrading and declassification, with Confidential documents automatically declassified in six years, Secret in eight years, and Top Secret in 10 years. Only four specific categories of information may be exempted from the General Declassification Schedule. The Order established a series of controls over what material is classified, who can classify it, and for how long. Let me note these controls:

- Officials with classification authority must be designated in writing by the head of their department or agency, and the list must be updated and submitted to the ICRC every three months.
- The classifier of a document must be identified on the documents. He is held personally accountable for the decision to classify any document on which his name appears as the classifying authority.
- The classifier is subject to sanctions for abuse.
- Top Secret classifying authority is limited to senior departmental officials and only these officials may exempt a classified document from the General Declassification Schedule.
- Departments must establish a data index system for retrieval of selected categories of classified documents which have permanent retention value.

Through tightened control over original classification and the introduction of the General Declassification Schedule, the Executive Order dealt with information that is currently being created and classified. But what about the hundreds of millions of classified documents that have been accumulating over the past 50 years? We estimated a year ago that the National Archives possessed over 160 million pages of classified information just for the World War II period, and several times that many for the post-War years. The new system was also designed to deal with this problem. Several provisions in the Executive Order relate to such older documents. One such provision is that classified documents 30 or more years old will automatically become declassified after a review directed by the National Archives. A Declassification Division, consisting of about 100 persons, has been established within the National Archives to conduct the review of records as they become 30 years old. It is possible that some of these 30 year old documents may be exempted from declassification, but this can happen only if the head of the agency or department which originated the document personally authorizes and justifies its exemption. Our best estimate is that the review of 30 year old material for the World War II period will result in the release of 99 percent of the documents.

In addition, material which is not yet 30 years old but is at least 10 years old is subject to a request for mandatory review by a member of the public or a department of Government. To initiate a mandatory declassification review request a member of the public must identify the document with particularity and the department must be able to retrieve it with a reasonable amount of effort. Definitions of particularity and reasonable effort are, of course, difficult to determine. In practice, however, the agencies seem to be interpreting these requirements generously. And adverse decisions can be appealed first to a Departmental Review Committee and then to the Interagency Committee, if an original request for declassification is denied.

Finally, for the first time a method was established to declassify material which was classified by a President, his White House Staff, or a Presidential Committee or Commission. Previously, Departments were reluctant to make a decision to declassify something they had not originated, even when the information fell within their area of competency. Now, through the provisions of Section 11, the Archivist of the United States is given the ultimate declassification authority after consideration of the donor's deed of gift and after consultation with the agency of primary subject matter interest. This provision of the Order has proved to be a major breakthrough in the declassification of material held in the Presidential Libraries as well as of material in the National Archives.

The changes in the classification system that I have outlined went into effect just over a year ago. Since that date substantial progress has been made in building the framework for a workable classification and declassification system.

During the year, the Interagency Classification Review Committee has emphasized the development of sound procedures for dealing with security classification problems and the establishment of a viable reporting system for evaluating departmental classification programs. Specifically, the ICRC has focused its attention upon reducing the number of Government officials with classification authority, review and approval of departmental implementing regulations, establishment of a quarterly reporting system, implementation of the data index, and education of Federal employees on changes adopted by the new Order. Since June 1, 1972, the number of officials with authority to classify information in the Federal Government has been reduced by 63 percent (exclusive of CIA which has reduced the total of classifiers by 33 percent). The number of officials with Top Secret classification authority has been reduced by 71 percent. (CIA has reduced Top Secret classifiers by 83 percent.) We anticipate that further reductions can be made during the next year.

In the area of declassification, the National Archives and the teams from various agencies have succeeded in reviewing for declassification some 40 million pages of material from the World War II period. In addition, during this period 350 mandatory declassification review requests were received by the various agencies. One hundred and ninety-seven of these requests were granted in full, and 26 in part; 79 were denied in full and 48 are pending action. Among the requests granted were those for the release of papers relating to the Abel-Powers exchange, the Adenauer visit to Moscow in 1947 and the release of the RB-47 fliers by the Soviet Union in 1967. In addition an appeal to the Committee for release of the Gaither Report of 1957 resulted in its declassification and release. Some Government departments have initiated their own review of existing classified documents to declassify those which no longer require protection. Of particular significance are the projects of the Atomic Energy Commission at Los Alamos Scientific Laboratory and the Department of Defense in its industrial security programs. We realize that the provision for mandatory review requests will not solve the problem of large volume declassification. Nevertheless it can be a useful tool in the hands of scholars, historians, journalists and others who can focus on identifiable documents.

The Executive Order and the NSC Directive provide a sound framework for an enlightened and reasonable approach to the Government's classification program. After one year, the Committee feels that significant progress has been made. However, we all realize that we are dealing with problems that have developed over a long period of time and that more than one year is needed to carry out changes as extensive as those included in Executive Order 11652.

A decade ago I doubt if anyone could have foreseen the changes that have taken place in the area of classified documents. What does it look like ahead? What will the world of classification management be like in another decade or so—say in 1984?

Prophecy, I realize, is a dangerous business, especially in the field of public policy, where the unforeseeable has a way of undermining even the most cautious prognostications. But, with all the risks, a look ahead is probably worth the effort.

What is likely to occur?

For one, thing, I do not believe that the present system will remain unchanged. I think we are likely to see further substantial modifications in the system of classify-

ing and declassifying documents. Moreover, I believe those changes will continue to be in the direction of the right to know. If the Government's experience under the Freedom of Information Act is any guide, I think it most likely that the requests for mandatory review will number in the thousands each year rather than in the hundreds as today. Finally, it seems to me not unlikely that there will be a much more stringent control over a smaller number of classifiers and a significantly smaller body of classified material.

Some of you may find these prospects frightening. Some may feel that the possible changes would still not have gone far enough. In any case, should such changes take place, we will all be faced with a good many problems, and those in the field of classification management will be called upon to bring their experience and their expertise to bear in solving those problems.

Twenty-odd years ago "containment" became and long remained the watchword of our foreign policy. Its diplomatic usage as circumstances in world affairs have changed has declined, but it is a useful word, and I suggest that it now become a new kind of watchword, the watchword of our classification policy. Uncontrolled secrecy can present a deadly danger to a democratic society. It can damage, perhaps beyond repair, the very foundation of that society, namely the ability of its people to control their own destiny. The *containment of secrecy* is our goal. It will not be easily achieved, but with good will and common sense, and with the professional dedication of men and women like yourselves, it will be achieved. ■

DISCUSSION OF SECTION XI–NATIONAL SECURITY–PROPOSED FEDERAL CRIMINAL CODE

Mr. Walter G. Fenerty,
Office of the Judge Advocate General, USAF

Mr. Robert L. Keuch,
Deputy Chief, Appellate Section,
Criminal Division, Department of Justice

Mr. Robert C. Maynard,
Associate Editor/Ombudsman,
The Washington Post

Mr. Fenerty: It's a pleasure to be here and especially to see all of the people who are concerned with this often unappreciated subject of the classification of papers of interest both to the Government and to the public. The subject matter, withholding or disseminating information, as some of the speakers have pointed out, has become particularly crucial of late and it is gratifying to note that so many professionals are involved in acquiring what additional information is available, what additional education is available, in order to pursue their task effectively.

All of us who work in the U.S. Government are public servants and it is a difficult task to decide, I'm sure, when your position as a servant of the public causes you to mark some particular item of information as not available to that public that you are serving.

I saw the other day an item to the effect that someone was exploring the possibility of classification by computer. Unfortunately, I don't know enough about computers in general and that project in particular to know any of its merits; but I can assure you that I'd be much happier to have your expertise on the classification question than that of any computer.

To lead off and to return to the actual legislation which we are concerned with today, I begin by narrowing, I suppose, our attention. Instead of all security offenses, which I'm sure you know embrace sabotage, embrace some matters affecting military personnel and so on, you will be concerned with the information disclosure facets in particular.

The present law, as again I'm certain most of you know, does not deal generally with classifying information as such. The present criminal law for the most part deals in specific categories of information, information which although somewhat differently described in various places is categorized as national defense information–information affecting the national defense.

What is the relationship between that and classified information? Generally there is none. There is no direct connection in the law between classification and the criminal statutes punishing the misuse of information affecting national defense generally.

Having said that, I have to back off. One of the serious problems in drafting any statute to describe information which should be subject to punishment for misuse is the description of it in terms of categories that could be understood by people who deal with it on the street; that is, the public in general, the man who is in the Government as an employee, or who comes in contact with it in his other occupation, perhaps as a journalist.

The status of the information affecting the national defense, which is not classified and is subject to punishment for misuse, is–I think I can say without passing immediately the question to my colleague, Mr. Keuch–uncertain. There have been few, if any–I know of none–prosecutions for a violation of a criminal statute involving the misuse of information affecting the national defense which was not in fact classified, with one exception. Then, that one exception resulted in a reversal. So I can say that I know of no successful prosecution for misuse of national defense information that was not classified.

The existence of only an interpretative gloss, as I would call it, on the category of national defense information which would restrict it to information which had been classified by some agency of the executive creates problems. So long as it is unclear what information is within the category covered by the law, few people will know what they can do with it–with information which appears to affect the national defense in some way.

Almost any information dealing with military matters–for instance, the location of the Pentagon–will affect, in the broad sense of the word, the national defense. I do not think there is any quarrel with the proposition that no one should be prosecuted for disseminating the location of the Pentagon.

On the other hand, there is no doubt that we do have something in mind when we talk about information affecting the national defense, some form of information which we do not believe should be available to those outside of our nation who would harm our nation; and

perhaps not even to some who are within the nation who would nonetheless, in the judgement of--not getting into the philosophy behind it--at least the vest majority of the citizens, would harm the nation as a whole.

The two major statutes that we now have on the books dealing with information affecting national defense deal with it in terms of the mental state of the persons involved, the communicator, if I may use the shorthand term for it. If I may, I'd like to bring them out and read those.

The most severe of the statutes dealing with information disclosure is the espionage law. It deals with the national defense information by punishing actions taken by a person who has the mental state: with intent or reason to believe that the information would be used to the injury of the United States or to the advantage of a foreign nation.

That is paralleled to a somewhat lesser extent by a similar statute that goes into more detail. I'm not going to read it all because it would unnecessarily delay the program. But by and large it can be summed up by talking about the intent or the criminal mind of the individual who deals with the information. That's one way of dealing with the problem.

At this point I'd also like to touch upon the two present versions of the proposed revision of the law. The first is a revision proposed by the Senate Subcommittee on Criminal Laws and Procedure of the Committee on the Judiciary. That deals with the problem in two ways.

In the first of the two, serious offenses, it preserves the mental state requirement. This is the basic espionage law. The bill I'm referring to is numbered S-1. The offense again is espionage, and in its somewhat complex numbering it's Section 2-5B7.

In that section the crime is contingent upon a state of mind as follows: with knowledge that the information is to be used to the injury of the United States or to the advantage of a foreign power; or with intent that it be communicated to the enemy and in time of war communicates the national defense information.

That is the most serious of the crimes that S-1 proposes to substitute for the present offense of espionage and its lesser offenses.

It too has another offense, however. That deals with the problem by punishing harmful use, simply communicating the information.

The mental state here is a lesser one, really summed up as knowingly. As most of the categories, it involves a knowledge of the probable result of its being communicated. The requirement is that the information be used in a number of ways, in a manner harmful to the safety of the United States.

In this case the problem of the location of the Pentagon is solved, because no one could be punished for having an intent to use that information to the injury of the United States. I believe it's safe to say communicating that information would never be in a manner harmful to the safety of the United States.

H.R.-6046 or S-1400, which is the version proposed by the Administration, deals with this problem in a slightly different fashion, although it again preserves the mental state requirement to separate the good disclosure of defense-related information from the bad disclosure. In the Administration version the intent is that the information be used or with knowledge that it may be used to the prejudice or safety or interest of the United States or to the advantage of a foreign power.

That is basically all I'd like to say on that at this time. I'd like to save for Mr. Keuch the opportunity to expand on the Administration version in a little more detail.

The other aspect of the separation of the good information disclosure from the bad information disclosure in matters relating to the national defense deals with what is in fact classified. And the law does now deal with classified information as such in two and a half categories, let's put it that way.

The two clear categories are the communications information, the information relating to communication surveillance by and large, and I'm sure you are familiar with that because many of you deal with that type of information. That particular prohibition is preserved in both the Senate Subcommittee version and the Administration version; although the language is a little bit different in each one, by and large the definition remains the same. They have been carried over and just slightly reworded. That information then is basically unaffected.

The other section that now deals with classified information as such is the communication by a public servant to a foreign agent.

In the Senate bill, the Senate Subcommittee bill, there is no comparable provision as such. There is no provision dealing with communication of classified information as such by a public servant.

In the Administration version there are several corresponding provisions which are somewhat broader. The public servant is put to a slightly increased burden, put on a slightly more elevated platform by the requirement that he not communicate the information to anyone--classified information--without authority, and the category of public servant is basically expanded to include information which a contractor obtains by virtue of his position. The public servant is obligated to take care of all classified information. The contractor or former public servant is obligated to care for all information which he obtains by virtue of his position; or at least he is subject to punishment if he does not.

Now, I mentioned there was another half of a section that dealt with this. There is a misdemeanor prohibition in existing law covering the photographing, mapping, sketching and the like of certain military installations and equipment, if it is designated by the President for that protection.

Those sections have been implemented in such a way that theoretically they would apply to classified information. They are carried over into both versions of the revised criminal code, but I know of no one who actualiy believes that it would be applied to matters such as the Ellsberg Papers--well, theoretically, they were reproduced from information that would fall in that category. Again, I think I'll have to pass that question on to Mr. Keuch.

I would like to just mention two other areas that are not covered. One is atomic energy. That basically is untouched by any proposed revision of the code. That would remain essentially the same. In the category of information which would be covered by either version of the proposed revision, Restricted Data under the Atomic

Energy Act would be categorized or described as being information affecting the national defense. Again there is a slight difference in the language but basically it would be the same.

Finally, from the standpoint of the lawyer, all of this matter would be affected by what could be produced in court or what would have to be produced in court. That is not affected by either bill in those terms. It would be affected from the standpoint of the drafting of the language. If the language were drafted in terms of requiring production of classified information in order to establish one of the elements that the statute has, then of course the prosecution could not proceed without disclosing it. But neither bill attempts in so many words to deal with the problem of the procedure of proving the fact of any category or of identifying the evidence to be used. Both questions are being considered by the Congress at this time, but neither has reached the stage where you can identify or describe a position as the probable outcome.

I think at this point perhaps the best person to discuss the view of the criminal law revisions, the proposed criminal law revisions, that the public would take would be Mr. Maynard of *The Washington Post*—the representative of *The Post* interested in disclosure of the good information.

Mr. Maynard: I must make it clear that the view I present to you this morning is my own. It is not the view of *The Washington Post* necessarily. As the ombudsman of that newspaper, I get the right to have a view of my own without having it incorporated, shall we say, into the views of the institution. Obviously, there are a number of things about which we agree.

This area, this whole question of the recodification of the criminal code with respect to national security questions is one that I'm sure you know is somewhat confusing at this point.

There are before the Senate at least two proposals, S-1 and S-1400 also known as H.R.-6046, which attempt to make some changes in classification responsibilities both in terms of custodians of information and those who are allowed to receive it.

The reason it is confusing is that apparently not very many people agree on what all those revisions actually would mean. There are those who take the view that H.R.-6046 and S-1 in fact protect journalists to the degree that they narrow the culpability. And there is of course an equal amount of vehement argument that they do the opposite.

I would just like to take a couple of those revisions. When you compare the old Title XVIII, 798, which if you're familiar with it, more or less provided that whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes or uses in any manner prejudicial to the safety or interest of the United States or the benefit of a foreign government to the detriment of the United States then it goes through some very specific language as to the kinds of material it is discussing—i.e., the use of code or cipher. Quoting now from 798 of Title XVIII "the design, construction, use, maintenance, or repair of any device used or prepared or planned to be used by the United States [for graphic purposes], communication of intelligence of activities of the United States or obtained by the process of communicating intelligence in the communications of foreign governments. . ."

In the new language of H.R.-6046, a person is guilty of an offense as being or having been in authorized possession or control of classified information—and now I'll skip over—he knowingly communicates such information to a person not authorized to receive it.

And it goes on to establish that it is not a defense against prosecution under this section that the classified information was improperly classified at the time of its classification or at the time of the offense.

Now, let me just make a comment on how many journalists view that particular portion of this new proposed legislation.

It does seem to us that this becomes a kind of a catch-all for all kinds of misclassified information. You will hear discussion later on today of the Pentagon Papers and the propriety of the classifications that were involved. And I have myself from time to time been involved in situations where there were highly dubious circumstances surrounding the classification of given documents. I'm sure no one in this room would ever misclassify a document, and I start off with the assumption that you are not the objects of our concern in the news media. However, there have been instances—I'm sure you all know; perhaps you know more than I do—instances in which embarrassing materials are classified that had nothing to do with danger to the national security.

And I think it's important to enter one other observation at this point. When we speak of overclassification, as journalists, we are speaking of the need to inform the American people of that which we believe your fellow citizens and my fellow citizens should know about to make sound judgments that are necessary and vital to the operation of the democratic society.

I know of no serious-minded journalist who is interested in harming the national interest—that is to say, his own interest, the interests of his family, the interests of his community, the interests of his country. And I think that's important to bear in mind in this discussion. There has been some notion abroad in this land ever since the Ellsberg case that the news media were about the business of making all of our secrets known to all the world. And I don't think that is what we're about.

We're trying to find a sensible way to make a clear delineation between what is properly in the public domain or ought to be in the public domain and that which properly ought to remain secret. And it's clear in looking at the Ellsberg case, for example, that whatever else may be true about those documents, nothing about them was vital to our security in the same sense as knowing the design of a piece of equipment or hardware that goes into a missile or whatever or a satellite or the kind of technical data that we probably would all agree shouldn't be revealed to anybody. And I've never seen a schematic for some propulsion device that was supposed to be a secret only known to us printed in the *New York Times* or *The Washington Post* merely so we'd get a scoop. I mean that's not real, that's not in this world.

So I think we ought to have that understanding between us as we discuss this question.

The other things that I think we need to be very clearly aware of is that from the journalist's viewpoint

there is entirely too much government regulation of information, not just at the national level; it is going on at the state level as well. There are a number of cases across the country, especially in California, where reporters are being prosecuted for printing material that a state government considered to be intellectual property in the same sense as S-1400 attempts to define government intellectual property which may not be improperly communicated.

What we see is a pattern that is disturbing to us as American citizens, and it is a pattern in which government regulations and government legislation seems to be intended to blanket whole categories of information which we think belong in the public domain.

I'm very interested in hearing Mr. Keuch so I'm only going to make one more observation for now—if I have another opportunity, I'll go on.

But a couple weeks ago the Attorney General went before the Government Operations Subcommittee headed by Senator Muskie to discuss this legislation. At that time he said that in the draft he found a number of areas where he thought the language was sufficiently emphatic as to conceivably affect journalists in the pursuit of their duties when in fact that was not his understanding of the intent of the legislation. I have the transcript of that conversation and I'll be happy to share it with you if time permits.

But I think it's important to note that because it goes back to what I said at the start. This is a very difficult area in which to legislate sensibly. It may be almost as difficult as trying to legislate or rule in the area of obscenity. I hesitate to make that comparison, but I think it's worth noting that a Supreme Court Justice once said that he didn't understand what obscenity was in a technical legal sense but he recognized it when he saw it. And I think the same may well be said for some of what are now known as secrets: that they may be or may not be legitimate secrets but we frequently don't know that until we've had some opportunity to examine them.

How we do that in the light of this new legislation which almost sends a reporter to jail for even smelling a classified document is a question I think we'll have to somehow sort out. I'm sure that Mr. Keuch will be more than able to set me right anyway from my misgivings about this package of legislation.

Mr. Fenerty: One question: did you have the same reluctance to see enacted the version of the proposed revision to the code that the Subcommittee has drafted as S-1?

Mr. Maynard: There is a feeling that S-1 is somewhat better, but as far as I'm concerned I think that of the three possibilities now before us—798 and 9, 793 and so forth, of existing Title XVIII as now known, H.R. 6046, and S-1—most journalists feel most comfortable with the existing legislation.

Mr. Fenerty: Perhaps before we return to the actual text of the statutes as they are proposed to be amended and the few provisions that are pending, I should mention a few things that occurred to me subsequently.

First in that these two bills, for that matter the criminal law with which they would deal, are not the only legal matters which affect the release of information by the Government to the public generally, which affect the obligations of the Government to make material available.

Perhaps the obvious thing is the so-called Freedom of Information Act, the requirement that the Government make information available generally with certain exceptions. The proposed amendment of the criminal code is not going to affect directly the question of whether someone in the position of Mr. Ellsberg can be tried for one particular offense or another. It may, because of the way it is drafted, affect a person's decision to release the information; have a collateral effect on it. But not in so many words—it is not drafted in those terms.

Someone was asking about the rules of evidence. As I indicated at the end, those are also not directly affected by this proposed revision of the criminal code. Indirectly they may be affected because of the way the amendments are written. At trial, the statutory prohibition will determine what evidence is needed and the rules of evidence will determine how the offense can be proved. The rules of evidence are now before the House of Representatives for consideration. The proposed revisions of those will not take effect until there is a new law passed.

Leaving that aside, I'll pass on to Mr. Keuch to present in more detail the position and the provisions of S-1400, the revision of the code proposed by the Administration, that I referred to earlier. It is a more detailed version and for that reason I think you will profit from a discussion of it more so than from a discussion of S-1.

Mr. Keuch: I have a strong temptation here. By holding to our schedule I can speak for 20 minutes and cut off any criticism of the code. But I'll try not to do that. I think that the provisions of the codes and the differences between them and the differences between the recommended proposals and the present law will come clearer in discussion between members of the panel and with you ladies and gentlemen. So I'll try to be very brief.

On the other hand, I think it equally important that, in criticizing the proposals and in commenting on them, that we are very well aware of what it is that we are critizing and what it is we are commenting on. So I'd like to go through the provisions of the Justice Department recommendations as to the espionage sections of the national security chapter of the criminal code.

Where I think it's relevant I'll try to mention the corresponding sections of the Brown Commission report which is also before the House and Senate and of S-1 which is the third proposed version of the criminal code.

The provisions of present laws, on which Mr. Fenerty commented this morning, are carried forward to a large extent in the proposed criminal code, hopefully in much clearer language and hopefully in a much more concise and manageable manner.

The classic espionage situation, that is communication of information to a foreign government with intent to harm the country or to advantage a foreign government, which is now carried in 18 USC 794(a) and (b) and 793(a), (b), and to some extent (c), is carried forward in the proposed Section 1121.

I might comment that I don't intend to give you chapter, verse, and text. I don't want to read the code to you. I refer you to the espionage sections of S-1400, they are 1121 to 1126.

And as just noted, 1121 is the classic espionage situation. Sections 1122 and 1123 carry forward those provi

sions of present law which have to do with other activity which could result in compromise, both intentional activity without the intent of transferring it to a foreign power, and negligence or gross negligence or other activity which could result in compromise. Thus 1122 and 1123 reenact the present 18 US 793(d), (e), and (f). Section 1124 is the provision relating to classified information; 1125 is the provision relating to the receipt or obtaining of classified information by a foreign agent. I will discuss these latter sections in greater detail later; they are based on 50 USC 783 and 18 USC 798 that Mr. Maynard mentioned this morning.

1126 is a definitions section that applies to all the other provisions. I'll also discuss that in greater detail.

I would also like, at the end of reviewing what are in these proposed sections, to discuss with you the concept of information relating to national security because that is a phrase that will be repeated a number of times in the proposed code.

And in discussing, in greater detail, the two of the provisions that have gotten the most comment and criticism—that is, 1122 and 1124—I would also like to explain some of the general interpretation rules of the criminal code.

1121, again, is the classic espionage situation. It makes it a criminal offense for an individual knowingly, and with the intent that the information be used to the prejudice of the safety of the United States or to the advantage of a foreign power, or with knowledge that it may be so used, to do one of three things:

- To communicate this information to a foreign power;
- To obtain or collect information with the intent that it be so communicated or with knowledge that it may be so communicated;
- To enter a restricted area with the intent to obtain or collect information for communication to a foreign power, or with the knowledge that it may be used for the benefit of a foreign power.

Entering the restricted area covers some of the matters Mr. Fenerty mentioned this morning, that is photographing installations and the rest. Those items are dropped out of the proposed code, and entering the restricted area with the necessary intent, as I mentioned, is in the classic espionage statute.

You might see that, by combining 793 and 794, we have made those steps that are, perhaps, preliminary to the actual communication to a foreign agent if done with the necessary intent and the necessary purpose, commensurate with and described in the same manner in terms of the same statute as the actual communication. As a practical matter, that's done under the present statutes, because of the penalty provisions, and also the fact that, generally, the obtaining and collecting was but a step in a conspiracy to communicate information to a foreign government.

So, 1121 is the classic espionage situation and I might point out has received very little criticism or comment from even those people who are most critical of the proposed code.

In Sections 1122 and 1123, again, we get into those circumstances where there are acts that are not done with the intent to communicate to a foreign government, but which may result in compromise. And the first of these, as I mentioned, concerns intentional communication. Section 1122 makes it an offense for anyone to knowingly—*knowingly*—communicate information relating to the national defense to a person not authorized to receive it. Section 1122, as I mentioned earlier, I might say reflects 793(d) and (e) at the moment in the present code.

Section 1123 carries forward those activities that are perhaps not intentional but also could result in compromise; and it has three provisions.

The first of those in that anyone in possession of information relating to the national defense who recklessly (and if I may be permitted a non-lawyer's comment for a moment, recklessly is defined in the statute terminology as the grossest negligence; you have to have knowledge of the circumstances, you have to act in such a manner as you should have actually no concern about the results of your actions, etc., etc. Recklessly is defined very broadly, that is, in the sense of the knowledge you must have and the type of activity that must go into it. It's the grossest of negligence, if I may put it that way) who recklessly permits the destruction, loss, theft, or unauthorized communication of information relating to the national defense.

The second area covered by 1123 is an individual in authorized possession. An individual in authorized possession is guilty of an offense if he does one of three things:

- Intentionally fails to deliver upon demand information relating to the national defense, demand being made by an authorized person;
- Knowingly fails to report a theft, loss, destruction, unauthorized communication of national defense information;
- Recklessly violates any duty that is imposed upon him, or her, by statute, executive order, or rule or regulation thereunder designed to protect national security information.

I supposed that this subparagraph does not have close comparison in present law. However, 793(f) and 793(d) and (e) in some respect do cover this. But this does provide for an offense by an individual who recklessly violates a duty imposed by law for the protection of national security information.

The third provision of 1123 applies to those who are in unauthorized possession of national defense information, and, here, they are guilty of an offense if they knowingly, *knowingly*, deliver the information to an individual not authorized to receive it.

Section 1124 is the classified information section. It provides that anyone who is in authorized possession of information or who has had authorized possession of information, either under provisions of law or because of their position as a federal public servant, who communicates classified information to an individual not authorized to receive it is guilty of an offense. It also provides that the propriety of the classification, either at the time of the original classification or at the time of the offense, is not a defense in a criminal trial for that crime. It further provides, however, that no one can be prosecuted under the section as an aider or an abettor or as a conspirator. In practical terms, this means that the individual who received the classified information and then makes some further or future communication of that

classified information cannot be prosecuted under Section 1124. It's only the individual in the position of trust, someone who has the information in an authorized manner, lawfully, who makes a communication who can be prosecuted for communicating classified information.

I'll come back to that in more detail. We think that in some ways this goes beyond present law. We think in other very significant ways it tightens up present law.

1125 is a counterpart. It covers the individual who is a foreign agent or an agent of a foreign power who obtains or collects classified information. This section has received no criticism whatsoever.

1126, as I mentioned, is a definition section. I won't go through them all. Classified information is defined generally as information whose dissemination has been restricted under executive order, or law, or rule or regulation thereunder, for reasons of national security.

National defense information is not defined. I would now like to discuss the phrase "information relating to the national defense," because it runs all through current law and, of course, throughout the proposed code.

There was a very, very strong effort made to codify into the code a definition of national defense information. But perhaps it is a little bit like the obscenity problem. That is, we know what it is. I think all of you can tell me that you know what national defense information is, if you have to deal with it day after day. But to sit down and write a statute that will be good, not for today, and not for a month from today, or not a year from today but for--well, presently our statutes, many of them, have been in existence for 50-some years. And there was a battle between whether or not we could, in statutory language, incorporate all the concepts of "information relating to the national security," and at the same time leave the flexibility to the courts and to juries to apply those standards to unforeseen situations.

We opted not to define the phrase--I think we had to; I don't think there was really a choice; we found it was impossible to define all the concepts, all the litigative gloss, that is, the case decisions, that have interpreted the phraseology of information relating to the national defense.

So we did not define it. What we have done in Section 1126--it's 1126(g)--is to state that information relating to the national defense is information, regardless of its origin, which includes information relating to--and we list a number of categories; I think we refer to those as illustrative subcategories. If you will read that list, it includes military plans, military statistics, military weapons systems, and the rest, also including foreign relations affecting the national security.

We purposely--*purposely*--carried over into the code the legislative history and the case history of "information related to the national defense." That's very important. There are two cases that are very important. I hate to be a lawyer and cite you cases, but the first is *Gorin vs. United States* which is in 312 United States Reports at page 19.

Gorin defined national defense information as a broad concept of broad connotations, referring to the military and naval establishments and related activities of national preparedness. That concept is purposely and intentionally carried forward into the present code. You would have to satisfy that concept of national defense information in any prosecution under the proposed code, because we have carried forward the identical language and the legislative history has been abundantly clear that we have intended to do this.

Another very important case is the *Heine* case, which is a Second Circuit case, 151 Federal Reporter 2nd series.

Heine is important because it has some concepts of defense that are available to the offense of the communication of information related to the national defense. Those three defenses briefly are that the information is already within the public domain; that is, it is lawfully "accessible" from legal sources; two, that the executive had made no effort to control the dissemination or disclosure of the information; and, three, that the information has been officially disclosed by the executive.

Mr. Fenerty mentioned this morning that there has not been any successful prosecution that he knows of in a case involving "information relating to the national defense" when the information was not classified. One of the reasons would be, of course, that one of the defenses is that the executive had not taken any steps to control the dissemination for the purposes of national security. If the document is not classified--that will be only in very, very rare situations, I think you'll agree, probably the only exception would be someone who is working in a lab or working on projects that are classified and comes up with a brand new concept or brand new idea that will be "classified" as soon as it is possible to get it into the system, but at that point it is not.

So one of the defenses to unlawful communication of national security information would be that the executive has not made any effort to restrict the dissemination. And, of course, as Mr. Fenerty pointed out, there has been no successful prosecution when the information has not, in fact, been classified.

One final concept on "information related to the national defense" comes from the proposed statutory language. In the description of national defense information, it provides a series of things as I mentioned, the last category, 1126(g)(10) says: during times of war any other information relating to the security of the United States, which does certain things--the point being that that phraseology is intended, and does, modify all the above concepts. We also make it clear then, I think, that the "information related to the national defense" must be of a type that affects the national security of the United States.

Now, that's a brief thumbnail sketch of Sections 1121 through 1126. I hope I've treaded the middle ground between giving you too much and giving you enough to understand the provisions.

If I may briefly--I'm going to save time for comment--go back just to Sections 1122 and 1124.

1122, again is the communication by anyone to a person not authorized to receive it of information related to the national defense. I would like to point out that the statute makes it a knowing communication. And under the statutory interpretation, rules of the proposed code--the culpability section of the proposed code--when you provide a level of culpability such as knowingly or recklessly or the rest, it implies, unless the statute makes it clear otherwise, to every element of the offense.

What that means in 1122 is that the crime is for a person to knowingly communicate to a person he knows is not an authorized recipient of information which he knows is information related to the national defense. The knowing requirement goes to all three elements of the offense.

Quite frankly, to be candid again, we expected some comment on 1124, the classification section, which I will briefly discuss in a moment. We think it does depart in some degree from the present law. We did not anticipate any comment or criticism of 1122. We felt it was a fair reenactment or recodification of 793(d) and (e), which does provide that it's a crime to communicate to a person, not authorized to receive it, certain specific types of matters related to the national defense; or also to communicate information related to the national defense which information the possessor has reason to believe could be used to the harm of the United States or the benefit of a foreign government.

I would point out that in the *New York Times* case, Justice White's opinion, and a number of other Justices joined in that opinion, I think a good majority, pointed out that that statute, 18 USC 793, was interpreted in just that way. Under prior law, existing law, it is a crime for an individual to communicate specific types of information such as documents, books, code books, maps, photographs, etc., relating to the national defense to an individual not authorized to receive it.

The last category, information relating to the national defense, which information the possessor has reason to believe, etc., was added in 1950 or 1951 I believe, and the additional test of having reason to believe that it could be used to the advantage, or harm the United States, was put on because it was a catch-all category of information. When you have a book, map, or document generally, as we have already discussed, that book, map, or document has some indiciation on it that it is related to the national defense. However, oral information, information that you obtain in some other manner than in a physical shape, may or may not, so the additional test was put on.

However, 1122 of the proposed code, again, would require the individual who communicates must do it knowing, knowing that it's information related to the national defense. And that phrase, as I have indicated, would include all the concepts of the previous cases and, very importantly, all the defenses of previous cases.

Section 1124, the provision for communication of classified information—I mentioned it had some predecessors in the present law. It does. It has three really. The first two are really more relevant: 50 USC 783(b) makes it a crime for any—*any*—Government employee to communicate classified information to an agent of a foreign power or to members or officers of certain Communist organizations which, by definition, would have included a lot of American citizens—the organizations included Communist-front, Communist-infiltrated organizations, etc., etc., and the very concept of those organizations is that they were created to get support of innocent and unknowing citizens.

18 USC 798, as Mr. Maynard mentioned this morning, provides for the communication of a specific type of classified information—communications intelligence information—by anyone, to anyone not authorized to receive it. And he seemed to indicate in his comments that it was very specifically defined and that it was a narrow category of information. I don't quite agree, because in the definition of the statute it provides that communications intelligence information includes information obtained from our communications intelligence procedures.

I'm sure there are people in this audience who can speak with much better knowledge and ability than I can to our attempts and our successes in obtaining information from our enemies—perhaps in cases from people who may be our enemies at some point or were at one time—through our communications intelligence methods. So the category of information is really not that limited. It would, for example, include information intelligence estimates if they had information that was obtained from communications intelligence sources.

The third one I will only mention briefly. The Atomic Energy Act provided that anyone who communicated Restricted Data information was guilty of an offense. And we would have taken the position in a prosecution that there is no need to show anything other than the information actually transmitted had in fact been classified as Restricted Data.

Now, under those statutes, I'd like to point out that 50 USC 783 says: any Government employee who transmits any classified information to a specified class of people—agents of foreign powers or members of certain Communist organizations; 798 says anyone—*anyone*—who communicates a specific type of classified information to anybody is guilty; and the Atomic Energy Act made it anyone who transmitted or communicated a specific type of classified information—i.e., Restricted Data—to anyone was guilty of an offense.

Now what the proposed code does—and like lawyers we like to draw on the courts and the wisdom that goes before us as much as anyone else does; and those statutes have been in the courts once, in the *Scarbeck* case a few years ago. Mr. Scarbeck was a State Department employee who was being blackmailed by the Polish secret police while he was in Poland. He took out of the embassy some classified documents and permitted them to be photographed by the Polish police; and he was prosecuted under 783(b).

Now, at trial, we established that the documents had been classified by the Ambassador, that his authority was in the executive order, at that time 10501, and they were classified pursuant to his authority. I don't mean that they were properly classified.

The contents of the documents were never made available to the defendant, to the jury, nor to the judge. On appeal, to the Court of Appeals of the District of Columbia—I might say one of the panels, that would fall, if we have to make a category or dichotomy, on the liberal side of the court, including Judge Bazelon and Judge Fahy and Judge Washington, I believe—they found that that prosecution was proper and pointed out that the reason 783 was constitutional and was valid was the fact that it was limited to a very narrow group of people—Government employees—who had some information as to their duties and obligations in protecting classified information.

They also pointed out that the Congress fully intended to permit a prosecution without violating the same

national security the statute was designed to protect. If the only way we can prosecute for communication of classified information is by disclosing in the criminal trial that very classified information it's rather an endless circle, isn't it? You'd have to violate national security to protect national security.

The Court sustained the statute. The concept was this is a limited group, and the rationale behind Congressional enactment of that statute was obvious, not to disclose the information.

Well, 1124 is also limited. It's even more limited. It's not *any* Government employee, or it's not, as 798 was, *anyone*, or the Restricted Data section, *anyone*. It's anyone with authorized possession.

Now we think that's a limited group. You don't get authorized possession unless you're pretty well instructed on the obligations. One of the questions that arises frequently concerns people in a position of trust. As stated before, the statute only applies to those individuals in a position of trust who violate that trust. It does not, I again say, does *not* cover the recipient of classified information. Bob is just not correct when he says 1124, if he's referring to 1124, would be a situation where even smelling classified documents would make him guilty of a crime.

However, under previous law, under 798, if it happened to be classified information such as communications intelligence, or under 50 USC 798 under certain circumstances, reporters or other recipients or intended recipients could have been prosecuted as co-conspirators, aiders, and abettors. So we think that 1124, in a very narrow sense goes beyond present law. That is, that it does cover *all* classified information—the unauthorized communication to anyone not authorized to receive it. On the other hand, it's narrower because it only applies to those people in a position of trust.

I think that I cannot fully discuss the present espionage statute, which covers pages in the present code. I again find it crossing the line between giving you too much or not enough to really make a judgment on these matters. But, one other point I might mention is that the problems 1124 is designed to handle, that is, the communication of classified information, which probably many of you know much better than I do, have been a matter of concern in the intelligence branch or intelligence field, security field, for many, many, many years.

783 covered Government employees, but there are a vast number of people under our industrial security program, under commercial contracts and the rest—as this group makes abundantly clear—who have access to some of our most secure and most sensitive information for the purposes of building weapons systems, designing weapons systems, designing defense strategy, and the rest.

There is no provision for an individual who had the information in that circumstance and transmitted it to someone not authorized to receive. So that someone who is 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.

Bob mentioned that in his opinion the matters and materials that were discussed in the Ellsberg trial to date were not matters that would affect—did not constitute information relating to the national defense. Well, if he were setting on the jury, that would be his right to say so. Because in a prosecution under espionage, whether or not the information relates to the national defense is a jury question. In those prosecutions we must—must under all the espionage statutes I'm talking about, except those relating only to classified information—we must disclose the very information we sought to protect, in order to prosecute.

A few years back we had a prosecution in New York where a sailor took five or six volumes of Secret radar documents, having to do with the radar system being used by the destroyers in the Sixth Fleet.

The Bureau was doing its usual fine job. We had a television camera in his office, we had surveillance outside, we had films of the individual removing the documents from the Top Secret safe—or Secret safe in this case—putting them in his car, driving to Narragansett, and there meeting with an agent of the Soviet Embassy in Washington, D.C., at which point he started to hand over the documents and was arrested.

Now, at the trial those radar manuals were declassified, as they would have to be under the normal espionage statute, so we could establish to the satisfaction of the jury that they were full of information relating to the national defense.

Let us assume, however, that instead of the radar manuals—which I think many of you will have to recognize, the radar systems of destroyers in the Sixth Fleet are probably because of the counter-measure systems that we have now, that our enemies—we're not sure—have, our radar systems are perhaps not that sensitive. Suppose it had been the concept of an entirely new device, something of which the concept was entirely new, and the same thing had happened: he had made contact with the Russian agent, he had attempted to sell, we had been able to arrest at the same time.

Everyone says that 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 the individual in a position of trust over that classified information without disclosing the very information you are seeking to protect.

I suggest that the information that can generally not be declassified for the purposes of trial is the most sensitive and the most important. And 1124 was designed to close that gap to reach only those people who are in a position of trust over the information.

Finally—one final comment—I think the tension between the press and the public and the Congress and the Executive on these matters is very, very important. If the Department of Justice or the prosecutors became extremely happy with the proposed legislation, Bob might raise some questions in his mind. I think if we proposed the statute and the members of the public and the press did not seriously question it, I think we might have some problems. I think that tension is inevitable. I think it's good. I think the give and take back and forth and the

criticism and comment may result in a better code. Perhaps this is the basis of some of Mr. Richardson's comments the other day which I will get into deeper if there are any questions about it.

Questions and Discussion

Mr. Fenerty: Mr. Maynard, you had a little briefer session previously than we had anticipated. Perhaps you had something further to say?

Mr. Maynard: I think I should say before anything else that in the three or four months, I suppose, since his proposed code became available, I have heard any number of discussions, summaries of the substance of this material. And I must say that even though I am not thoroughly persuaded on all of Mr. Keuch's points that this was surely the most cogent summary that I have heard so far, and I'm very grateful for it because I learned a lot in the process of that summary.

We were talking earlier about the possible vulnerability under one of the other sections, 1124 I believe. But I am very interested in getting Mr. Keuch's reaction to a question on 1122 in the new code, because I think this raises some of the problems that we as journalists have to cope with.

1122 you will remember is the section that requires knowledge of the communications, knowledge that the information relates to national defense, and knowledge that the person receiving it is not authorized to do so.

Now, I have a little summary here to which I would like Mr. Keuch's reactions:

That the existing law requires a showing that the information in question (a) relates to the national defense and (b) is of such nature that the possessor has reason to believe that it will injure the United States or aid a foreign nation if it is communicated to an unauthorized person.

No such requirement exists, as I understand it, in the Nixon proposal, and that the requirement is perhaps the basis for the Ellsberg defense; and that further, the *not authorized* in the new proposal is considerably more narrow than the *not entitled* in the existing law, and that anyone not specifically authorized by law under the new proposal may not receive defense information on pain of criminal penalties.

And here's the problem: allegedly one may be entitled under the existing law but not be authorized under the new law. If we get in this, we're not talking of the person who was originally authorized custodian of the information, but a legislative assistant in a Congressman's office could come upon the information, consider it to be vital, that it be released—under this proposal as I understand it, the legislative aide and conceivably the reporter who receives it from him would both be vulnerable for prosecution, whereas they would not have been under the previous law.

Mr. Keuch: I'd like to comment on that, if I can keep them all in mind.

First, I think there's a misunderstanding in the summary. If I recollect, I think that was a memorandum of Senator Muskie's, but perhaps it wasn't.

Mr. Maynard: No.

Mr. Keuch: First, it states the present law does not prohibit the unauthorized communication of information relating to national defense, unless you can show that the individual knew that it could be used to the harm of the United States or to the advantage of a foreign power. This is not so.

793(d) and (e), as I tried to mention, say: it shall be a crime—or however the phraseology is—for an individual to communicate specific types of information—books, documents, maps, photographs, code books, etc., etc.—the listed specific items, related to the national defense—semicolon or perhaps comma, I'm not sure—and then it says: or information related to the national defense which information the possessor has reason to believe could be used to the harm of the United States or to the aid of a foreign power.

Now, I'm not going to just rely on punctuation. The legislative history of the addition of the phrase, information which the possessor has reason to believe, etc., is so crystal clear that what Congress was doing there was engrafting the additional requirement that you show that the possessor knew that the information could be used to the harm of the United States or to the advantage of a foreign power—because information would cover oral communications possibly, would cover things that were not in a physical shape where they would probably have some indications they were covered.

I don't have to rely on my interpretation, thank goodness, because I can point to Justice White, Justice Berger, Justice Powell, and Justice Stewart and most of the other members of the Court in the *New York Times* case—*New York Times* and *Washington Post* case—which said that 793 was interpreted just that way.

I don't think that I should just rely on that. That would be the classic cop-out. In addition, it's not a question of whether or not we recodify present law. It's really what should the law be, I think, before we reform and recodify a code. However, I have a great deal of respect for the present law because it has been hammered out in the ovens of the democratic process and has been hammered out in the courtrooms across the country generally—the greatest respect. I don't think the Brown Commission has paid as much attention to it as we wish they had.

But the proposed code, I think, goes further in the requirement; that is, that there must be a knowing communication of the information, knowing it is related to the national defense. I tried to make clear that that knowledge would have to include all the concepts I talked about: that is, that it relates generally to the military establishment of the United States or the related aspects of national preparedness; that it otherwise affects the national security, etc., etc.

It's also very important that determination would be a jury question in 1122. The jury would have to determine, if it was the type of information and that the individual knew it, and he passed it on. The legislative aide in the example and the recipient will be just as guilty under the present law which has been in effect for 30-some years. I think there is some lesson to be learned in the prosecutive discretion that was used under a statute that has succeeded or existed for that long.

It would be a serious problem if you do not have a provision such as 1122 and have only the classic espionage provision, that is, communication intentionally to a

foreign power. We all know once we lose control of things we very often loss them entirely. If I cash my paycheck and I don't keep it in my wallet or in my safe but instead I put it out on the lunch counter downtown and come back a few months later, I may find that I've lost control of that money. The same thing is going to happen once we get information related to the national defense which escapes from the system.

Perhaps the legislative aide situation is a very good example. But if this is a departure from present—well, it's not a departure from present law, and I think it's a provision that is necessary.

Question: Mr. Keuch, this might be a mundane question, but the espionage laws in marking classified information, the contractor to the Government is required to put on a warning notice, whereas the Government is not. Can you tell us why that is done, what's the legal basis for that? Are you familiar with it?

Mr. Keuch: I'm familiar with the requirement, having been in the military myself. I would imagine that the difference is—well, I think one of the rationales behind it—I don't know; I honestly don't know. Maybe the rationale has been that the defense contractor is closer to an uncontrolled situation than the Government—for example, I wasn't too much concerned when my ship was a couple hundred miles at sea of getting classified information communicated to other people. When it got into port, it got to be a much more serious problem.

The concept may be—I honestly don't know—the concept may be because there's a lot more opportunity for individuals not having authorized access and so on to be somewhere within that range. Plus the fact, I suppose, that a Government employee who has classification authority, that's authorized to have classified information, generally stays permanently in that position; whereas, as I understand the industrial security program, an employee may work on a classified contract for McDonnell-Douglas, for example, for a five-year period and then for a five-year period work on something that's entirely unclassified, and then perhaps come back five years later—perhaps the rationale is that. I honestly don't know. That's just my guess.

Mr. Fenerty: You're referring to the lengthy wording that this is a violation?

Question: Yes. It used to be the Espionage Clause. I've often looked at the requirement within the defense contract as giving the person having access to the information notice that the material does contain classified information as the statement says. But it doesn't seem reasonable that the notice should be applied only to industry and not to Government since they both should have and be charged with that knowledge.

Mr. Keuch: I agree. Of course there are requirements in most agencies for periodic instruction to all employees who have access about their duties in handling this information—in fact, it's to all employees whether they have access in their daily jobs or not. Perhaps one thing is done one way and the other is done another.

We can control, I guess, our briefing session but I guess we can't be sure that industry will conduct those briefing sessions. Maybe that's it. I just don't know.

Question: I have a question for Mr. Maynard, if I may.

If in the course of your profession as a reporter you obtain information which you think may be classified—this is a double question—to whom do you turn for advice? And if it does turn out to be classified, what would you do with it?

Mr. Maynard: I think that frequently depends on the character of the information, obviously. One of the greatest problems is we have a flood of classified material in various agencies of the Government that leave themselves open to argument as to the legitimacy of the classification. I think that's one question.

You all may know about the incident that occurred out in Wisconsin where one of the military agencies set up a system for communication, and a newspaper out there wrote a story about it. When the story arrived in Washington for the inspection of the Pentagon it was promptly stamped classified. That's the kind of thing we have to be concerned about.

In answer to your first question, what would I do: my first attempt, obviously, as a citizen, if I think the information ought to be shared with others is to make some attempt to get it declassified. And if that proves to be impossible for whatever reason, then I suppose we discuss this with the agency involved and with the newspaper to try to arrive at some determination as to what ought to be done.

That's precisely what happened in the case of the Pentagon Papers. The editors of the newspapers looked at the documents and saw in most cases the material was old and didn't affect anything ongoing, and concluded there was no risk to the national interest that the coverage would reveal.

We'd go through this process. There are a number of things we do. You don't just walk in, see a document, and rush out and print it. No responsible journalist that I know of would do that.

Mr. Keuch: May I expand on that a little.

One thing I think I'd like to mention. I mentioned that 1124 was a reaction to a deep concern of the intelligence community for many, many years. In fact, back in 1956 the National Commission on Government Security, headed by various members of the American Bar Association and representatives of Government but mostly from the private bar and other things, had come up with this proposed code which made it a crime for anyone to communicate classified information to anyone not authorized to receive it.

The Department has always been strongly opposed to such a statute, thinking it has extremely serious First Amendment questions if not totally beyond the pale of the First Amendment.

One of the reasons 1124 came to culmination after this period of concern is one of the things you'll be discussing, I'm sure, and you are discussing, 11652, the Executive Order. I think there are some things in the Executive Order that made 1124 much more reasonable in our approach, particularly if limited to people of authorized possession; and particularly in fact that there are provisions open now to people to get declassification or to argue about over-classification. And perhaps more important, as we discussed at lunch, the fact is, if I originally classify a document that original classification follows that particular information I classify, not only in

that document, but in successive documents.

Now, if I would sit here and tell you I thought the Executive Order system and all the concepts of it are working 100 percent, I would be a fool, and I don't think I am. And I think I'm a good enough lawyer to know that there is much evidence around that says it is not working the way it should. We can bring horrible examples forward. They have been brought forward before and I'm sure they will be in the future. I suggest, however, that the answer to that is not to permit the individual in a position of trust who makes a unilateral declassification, if you will, of that information to escape all criminal responsibility; but rather to make sure that our system is an effective and good system. The system does at least now provide the review of classification; it provides for caring for, the accountability of that classification; and it does provide for at least administrative sanctions at this point for people who have misused the classification process.

One of the things Mr. Richardson, the Attorney General, mentioned in his testimony—I think one of the things that perhaps is implicit in the draft of 1124, certainly we had in mind as I just indicated in these provisions—was that it may be an improvement to make clear what is there by inference and by intent, to provide that there can be no prosecution under 1124 for communication of classified information if there is no administrative system open to the individual to challenge the classification of that system. That's one of the things that's being studied.

Of course that really is what would be present in the proposed code, what we intended, because the system is there in E.O. 11652. And if the system were not effective, if it were not working, Congress of course could deny us the authority of 1124.

Question: With respect to S-1, Section 2-5B7, harmful use, do you feel that that might have some overbreadth in its language; and also what constitutional standards do you use in drafting such legislation—compelling state interest vs. rational basis? Do you really consider that in drafting the legislation?

Mr. Fenerty: I could only speak for myself of course. I would like to think that we consider whatever we can lay our hands on—on anything that I deal with. Neither Mr. Keuch nor myself was responsible for the drafting of S-1.

The "harmful use" prohibition, I had neglected to mention, is in Section 2-5B8. The term "use" appears in 18 USC 798. I think it's also in one or two of the other laws. But the "harmful use," I assume, is the Senate Subcommittee's antidote to the overbreadth point, so to speak. By limiting the offense to harmful use I think they propose to avoid the claim that their provisions are overbroad.

Question: Knowing communications to a foreign agent vs. negligence in handling?

Mr. Fenerty: Well, as I would understand the S-1 provision, it would be intended to cover—well, the Government would have to prove harmful use in court as a matter of fact as an element of the prosecution's case. If it could not prove that the disclosure was in fact harmful—if they did not prove it was harmful to the United States, it would be no offense.

The difficulty with that—there are difficulties no matter which way you go, as Mr. Maynard and Mr. Keuch have pointed out here—is that it forces you to use 20/20 hindsight. The man who releases it and gets it right is home free and clear and everyone is happy. The man who guesses wrong, both he and apparently the national security suffer.

Mr. Keuch: I think there is also a little different answer too. That provision is comparable to 1122. It provides for communication of classified information relating to the national defense to unauthorized persons in a manner harmful to the United States. Probably that will be an objective stance. That is, in a criminal prosecution the proof would be that someone knowing that type of information, etc., etc., and the very fact that he took it outside the channels of control, if you will, channels of accountability and counting, and so forth, would be in a manner harmful to the United States.

But it also opens up the defense of, well, you know, "what I really intended was to benefit my country greatly by doing what I did."

As I mentioned, Sections 1122 and 1123 are designed to cover those areas of activity that do not have the "equal" intent to ultimate communication to a foreign government, but is activity that still could result in compromise.

Now the penalties are much lighter in 1122 and 1123 because of the difference in the intent. And I might also point out that the Brown Commission has a comparable position to 1122, without the addition in S-1 of, "in a manner harmful to the United States."

I think it might be very difficult as a layman to look at the Government's evidence and decide that that evidence was put in the case to prove it was information relating to the national defense and this evidence was put in to prove it was not in a manner harmful—one thing really does the other. I think this is why we felt, certainly that the drafters felt, that 1122, requiring knowing that this information was of that type, knowing communication to a person you knew was not authorized to receive it, really had a stricter standard than 793(d) and (e), and that the remainder of 793(d) and (e) which relates only to information in an oral manner is almost identical. I don't see how you can separate the two. As a practical matter, preparing a case like this, I can't see the difference.

Question: Is the continued and consistent use of the term national defense information here in the proposals a deliberate rejection of the term national security information as appears in 11652?

Mr. Keuch: It certainly is not an effective rejection of the term national security. We belive that the phraseology, information related to the national defense, is somewhat narrower than national security.

Again, up until the very last draft, the proposed Justice Department view did carry forward "information related to the national security," because it wanted to parallel the Executive Order. Our concept was we wanted to make very clear in the legislative history that we intended to carry forward all the concepts of present law, which seems to have worked in an admirable way. We have protected information and, also, I believe, have not steamrolled over other interests. We thought if we're going to make that clear in the legislative history, the

clearest way to do it is to say "information relating to national defense."

It's not a rejection of national security in the Executive Order, but it's an intentional, very definite attempt to make sure we're carrying forward the litigative history of the phraseology.

Now also there's good argument that national security in the Executive Order is somewhat broader than information relating to the national defense, because it does, I think, cover foreign relations information. National defense information in the proposed code would only cover foreign relations when it affected the security of the United States.

I might be hard pressed, to give you examples of something in foreign relations that you could not say would affect the security of the United States, but we think it's a narrower concept. There may be all types of tariff discussions and trade discussions and so on, that are not foreign relations that affect the national defense. We attempted very definitely to keep the proposed code to the concepts of the espionage statutes that have been in existence for 30-some years as far as the type of information that was covered.

We tried to be helpful by adding a list as I mentioned of illustrative examples of the type of information we're concerned about. We also provided for foreign relations information affecting the security of the United States. It wasn't a rejection as much as it was a clear acceptance of past law in this area.

Question: What were the intellectual criteria?

Mr. Keuch: Well, I'd like to say the people who wrote the theft statute should answer that for you.

Frankly, the theft provisions of the code, very briefly, were designed to cover the present 641; as Sandy mentioned, one of the counts of the indictment in the Ellsberg case was for theft under 641. And I frankly would have to let the people who drafted that answer.

I will say it was never intended to be considered in conjunction with or used with the espionage statutes, but only to codify what they thought was ultimate law under 641.

I think some of the cases where you can "steal" information without stealing the documents are things like trade secrets and the rest. They were not Government trade secrets. They were cases as to whether or not this is the type of thing to expect under common law and the normal concepts of theft can in fact be the subject of a theft.

I'd like to have the drafters speak for themselves, because I think the drafters felt if you take trade secrets out of a file cabinet and xerox them and put the originals back, it doesn't matter how you slice it and cut it, you've stolen trade secrets. I think that there was an attempt to codify what they throught was the present law.

Question: This is trying to bring copyright law into federal practice?

Mr. Keuch: I know that there was no attempt to put that into the control of classified information. I do know they felt there is a concept, and I agreed with some of the questions that came up this morning and some of Sandy's comments that the Government holds property and holds ideas and holds information for everyone, but everyone's rights can be diluted if that information becomes available in channels and areas it should not otherwise be available.

I think their attempt was to cover what they thought the present law covered. ■

THE PENTAGON PAPERS–WHO WON?

Mr. Sanford Ungar,
Staff Writer, *The Washington Post*

Newspaper reporters spend much of their time listening to speeches and only rarely are invited to give speeches. Usually the speeches we cover are far too long and too boring, and when you have a chance to speak yourself there are always two different ways of striking back. One is to give a long speech yourself in the hope that somebody in the audience has spoken one of the times when you had to cover a long boring speech; the other is to speak as briefly as possible and invite other people to make some more speeches but being in a position to control how long their speeches are.

I'll try to choose the latter course. I'd be very interested if at all possible in an exchange with people here on some of the subjects I touch on.

My subject is the Pentagon Papers, Who Won? I should probably begin by stating a few of my relative biases which are very strong biases and which I am not prepared to surrender at this point under any circumstances.

As a working reporter, as a journalist, I have I would say the strongest bias of all in favor of the public's right to know, and in favor of our role in the press, more or less–if you'll forgive the expression–as guardian of the public's right to know. I think and believe very strongly that we were established in that position by the framers of the Constitution in the First Amendment.

So I begin with the presumption, to take an example from the news today, that we are fully entitled to know that the military was bombing Cambodia in 1969 or 1970 when we were told that they were not. I start out with the bias that we were wronged by the Government, the people as a whole, the public interest was damaged by the people not being told the truth about what was going on in that particular aspect of the Vietnam War.

Another of my biases is that we cannot trust rules and regulations and individual people in positions of authority always to decide what we and the public are entitled to know. I operate, as most of my colleagues do, on the premise that we are entitled to challenge the whole notion of classification on particular documents in particular instances; that we as part of the public, as part of the public with a special role, are entitled to challenge those and question whether they have been accurate or not. I suspect that's a fairly strong and controversial bias in this room.

The third bias I suppose I should state is that I think that in some areas particularly, the rules have been written and the standards set altogether to an absurd extreme in favor of secrecy. I only recently learned–my current assignment has been to cover the Justice Department and

FBI—that all FBI files are classified and are kept secret for 75 years after their inception. I just can't think of anything more absurd than the notion that the FBI's work, any work it's doing cannot be revealed for another 75 years. That means that the first FBI files, when J. Edgar Hoover took over in 1924, still have another 26 years of secrecy to go at this point. I think that is just an outrage among many outrages that something ought to be done about.

Now that I've got the biases out of the way, I'll talk a little bit about the trial. I think though that those biases are relevant to what I have to say about the trial.

It has become customary and I think convenient and perhaps justifiable to look at the Pentagon Papers cases, the trial of Daniel Ellsberg and Anthony Russo, as a contest between two sides—on the one hand—I'd rather say on one hand, the Executive Branch of the Nixon Administration specifically, rather than the Government in general—the executive branch of the Nixon Administration, angry about the leak—concerned about their ability to operate in foreign affairs and conduct their business in private—on the one hand. And on the other hand, on the first level, Daniel Ellsberg, who felt for reasons that are probably familiar to most of the people in this room that he had a personal obligation to do something about the Vietnam War and to break what he considered a code of secrecy, and to a certain extent to atone for his own part in formulating the Vietnam War.

I think there's a third party in that contest, in that fight, and clearly that's the press. We were always in a very difficult and somewhat contradictory position throughout the Pentagon Papers litigation because—well, it would be bad enough for example to be covering a lawsuit against one's own newspaper, which is what I did in the summer of 1971, where there can be a presumption of objectivity but there could be no doubt on whose side the reporter stood, a situation like that.

But I think in the case of the Pentagon Papers trial the press probably stood not specifically on the side of the defendants but more or less as *amicus curiae* on the side of a public right to know. If it was not being eloquently and effectively defended by the defendants in the case, there was certainly a feeling that it was being attacked by the prosecutors in the case; so as *amicus curiae* not exactly in the middle, but very concerned with the outcome of the case.

I presume you all know the outcome of the case: Judge Byrne in Los Angeles dismissed the charges in early May not at all on the merits, nothing to do with the issues in the case itself, but on the basis of Governmental misconduct: the burglary by people dispatched from the White House at the office of Daniel Ellsberg's psychiatrist; secret wiretapping, the records of which had disappeared and were being kept in Mr. Ehrlichman's safe at the White House; all sorts of irregularities that one came to believe were out of the control of the specific Justice Department prosecutors who were handling the case but had been run out of the White House in one of its many extra-constitutional rolls over the past several years.

The defendants in the case, of course, proclaimed immediately that they had won when the case was dismissed. Ellsberg and Russo both called it a victory. They said they had been vindicated in their actions and that it was as good as an acquittal and they didn't have to go to the jury, because the Government had been shown doing the same thing against them, behaving in the same way as they felt the Government was shown to have behaved in the Vietnam War in the Pentagon Papers.

On the other hand, I think there were some people in the Administration or in the Justice Department specifically who felt that in a peculiar sense the Government had won (Government being used in this sense in the larger context, not the Nixon-White House, because it certainly didn't win), in the particular sense that the Federal Government is interested in protecting papers, secrets; and there had not been a clear verdict of an acquittal of Ellsberg and Russo. So that meant as far as the Government was concerned—and I expect we can anticipate people from the Justice Department saying so in court papers for many years to come—Ellsberg and Russo's conduct was not vindicated and they did not get a verdict from the jury that said this was all right. By the way, that is the verdict they probably would have had, had the case gone on, at least the way the jurors spoke to us after the trial, after the case was dismissed.

So the Government won in the sense that there was no clear mandate that went out from the trial which would unleash the feared flood of official secrets; many new revelations that would come from secret files.

One thing that should be said is that there were a number of things that probably arose out of the original leak of the Pentagon Papers, among them Jack Anderson's publication in January of 1972 of the documents revealing the truth about American positions in the Indo-Pakistani war; and probably some of the things that we have learned about Watergate, insofar as they are substantiated by documents, probably grew out of the precedent of the release of the Pentagon Papers. But still, I think the Government would be justified in saying that no flood was unleashed and that there was not a clear, and worrisome for the Government, precedent that came out of it.

Well, my view, as you might expect, being an objective reporter, is of course that nobody won; that probably in the long run no result from the trial was the best result.

I don't take that position in order to be a moderate with whom everyone can agree. But I take that position because I basically believe that the trial should not have taken place in the first place and that it would have been more in the public interest had the specific charges against Ellsberg and Russo not been brought and had the trial not gone forward.

Well, I lost on that one at various points along the way because the charges were brought and the trial did go forward. The second best I think in this circumstance was that the case was dismissed without a clear resolution of the issue.

That may sound a little inimical to the interest of the press, but I don't think it is. Because the position that I would like to test before you today is that this is the kind of thing and the kind of area which is best without specific ground rules, especially ground rules that grow out of a peculiar and specific case.

We learned that in 1971 when the Pentagon Papers were first disclosed and the only standard that turned out to be on the books was the case of *Near v. Minnesota*. In that case Chief Justice Hughes wrote a very eloquent

opinion which set apart some categories of information that could not be revealed, but even those categories were no longer very relevant. The question of when a troop ship sailed I think would no longer be considered that central an element of the national defense. At the same time that case of *Near v. Minnesota* grew out of a scurrilous newspaper printed in Minneapolis that nobody really liked, and therefore it was a bad situation from which to try to draw ground rules. But I'm saying that *this* was a bad situation to try to draw ground rules from as well, and that we would have been better off not forcing this case through the court process in an attempt to draw ground rules.

I think that over a period of years the thing that has worked best in terms of relations between the press and the Government in this particular area has been a kind of constructive tension. I think that's probably what the framers of the First Amendment had in mind, that there be people on both sides or all sides or many sides of these issues asserting their prerogatives, their influence over events, and that the press make its own attempt to do its job without having to line up a particular set of documents or particular stories against ground rules such as the ones that my colleague Bob Maynard and the others on the earlier panel were talking about that are proposed in the Administration's revision of the federal criminal law.

I would suggest that people in the press really over the years have, if anything, shown themselves too reluctant to break rules of secrecy. If anything, they have cooperated with Government secrecy in ways that have in the long run hurt the country.

The best thing that I can cite, and it's been cited many times, is the question of the Bay of Pigs invasion, where the *New York Times,* under pressure from the Kennedy Administration, having found out about the impending invasion of Cuba at the Bay of Pigs, agreed essentially to down-play the story. President Kennedy later said that he wished that the story had been blown in the *New York Times* because the invasion was such a disaster and the course of policy was such a mistake that the press could have served as an effective check on the Government in that instance.

There is no way that a situation like the Bay of Pigs invasion can be lined up against a specific set of rules and you can come out with an answer, right or wrong. I think you have to rely upon reasonable men who may differ honestly under circumstances and who can be counted upon to make good judgments from different interpretations of the public interest and even, yes, of national defense—which I think is a grossly misused term especially in something like the Pentagon Papers case.

I think that the results of a conviction or an acquittal in this case might have been very bad. Let me take the difficult one first: why would an acquittal possibly have been bad?

I think an acquittal could have been counter-productive to the press, *especially* to the press. I'm not talking about the selfish interests of Ellsberg and Russo. It could have been counter-productive for the press insofar as it probably would have unleashed a great deal of publication of new secret documents, additional secret documents. That could very well have resulted in a backlash in the Congress and among the public which would have led perhaps to very repressive legislation controlling what the press could do, and trying to bring the situation under control; the way Congress reacts to a Supreme Court decision it doesn't like—it sweeps too broadly and creates more problems in trying to solve the problems. I think the press could have been harmed greatly if after an acquittal in the trial any such backlash had arisen; and I suspect that it might very well have.

On the other side, the question of conviction, I think, would have set a disastrous precedent for the country and for the public interest. You're talking a lot in these proceedings about the Espionage Act and Section 793 of Title 18 and others.

There's another area of the charges that were brought against Ellsberg and Russo. One thing everybody said: if there was anything on which Ellsberg and Russo might have been convicted, it was theft. On the usual standards—and if the lawyers in the room will forgive me; I'm not a lawyer—but on the usual standards of proving a theft, it was clear and it was acknowledged that Ellsberg had removed these documents from the place where they had been kept and that he had copied them, that he had distributed them—and put them back, but that was a question over on the side. Another question over on the side was to whom the papers really belonged. Assuming for simplicity that the papers were Government property and that he did take them away and that he did commit a theft, it should have been very easy to convict him.

Well, according to one standard, that's not so terrible. This is a minor crime. Generally petty theft is not that serious and maybe it would have been worth it for Mr. Ellsberg. But the problem came in whenever the Government attorneys were asked in court to define what it was that the Government said had been stolen; because there had not been—in terms of classic theft, Ellsberg had put the papers back—so there hadn't been substantial deprivation of the use of the papers by the Rand Corporation or by the Government. Besides, there were other copies.

What was contended from time to time, and the prosecutors were never very precise about this and never pinned down on their exact theories, was that the information in the documents was Government property. I would contend that if we could convict somebody for stealing information from the Federal Government—and in this case from the Rand Corporation—that we have an official secrets act. And that that is a very serious thing, which the framers of the First Amendment never intended us to have and which in fact Congress has specifically refused time after time to pass.

I think I should end on this point and just among other things throw open to you the question of whether in the name of national defense and in the name of national security and keeping secrets within the Government, we really are prepared to declare that information belongs to the Government and that it is up to the Government and up to individual officers of the Government with all their flaws and foibles to decide what information the people *should* have, as President Nixon phrased it in a recent speech to the prisoners of war, and what information they *should not* have.

That, it seems to me, is far too important a matter to put into the hands of the Federal Government.

Questions and Discussion

Question: Do you feel the prosecution in this case called the best possible witnesses to establish the authenticity of the classification of the papers?

Mr. Ungar: Probably not.

No, I think that, judging it again from the reporters' point of view, if you will, from the point of view of somebody sitting in the courtroom and watching the proceedings from day to day, I think the Government's case was hurt substantially by calling only military people to talk about why the papers had to be classified. The point of view of the military is simply no longer accepted at this point of time in this country as being the definitive word on these matters.

There were other military men, in this instance of course retired military men, who disagreed with the Government's witnesses, and other people from outside from all different walks of life—professors and others—who also disagreed. I think that had a profound effect on the jury.

Question: When you combine this with the judicial misconduct of the prosecutors, couldn't you be led to the conclusion then that the Government did not want to win their case and felt morally bound to bring some type of prosecution?

Mr. Ungar: Well, if the Government didn't want to win this case, they sure fooled a lot of people.

With all due respect to Mr. Keuch and others in the Internal Security Section of the Justice Department, there are some areas which arguably were prosecutorial misconduct by the Justice Department in the case: for example, withholding damage reports, assessments of the importance of the Pentagon Papers. But that was an arguable matter. It was a question of law. I don't think it ever was completely resolved.

The real misconduct in this case was on the part of the White House and people operating for the White House. And one would have to say that if the people in the White House really wanted the Government to win this case that they did throw the case by their actions.

Question: The thought occurs to me that Ellsberg was guilty of the same thing that the Watergate defendants went to jail for: improper acquisition and dissemination of information.

Mr. Ungar: The Watergate defendants, I think, went to jail for burglary, illegal interception of communications, and conspiracy.

And conspiracy was also charged against Ellsberg and Russo but not burglary or illegal interception of communications.

Question: In your description of it there was a burglary involved in obtaining the information.

Mr. Ungar: But the Government in its wisdom did not charge the Watergate defendants for the theft. They charged them with burglary—breaking and entering—and with intercepting communications. And I think that therefore they had—Mr. Keuch and others in the room, correct me if I'm wrong—but I think a burglary case like that is a good deal easier to prove than a theft case such as was brought against Ellsberg and Russo. This is theft of Government property—Section 641, I think—which should be an easy thing to prove—in some ways should be an easy thing to prove. But I think the water was muddied considerably by the question of whether it was information or pieces of paper or what that was actually stolen.

Question: Isn't this what the Watergate people did?

Mr. Ungar: No.

Question: Stole information?

Mr. Ungar: They may have stolen information but they are not charged with that.

The Democrats of course brought a civil suit in which they may have said that the Watergate burglars stole information and papers from them, but there was no charge of theft against the Watergate burglars.

Question: What does a burglary constitute from a legal point of view?

Mr. Ungar: I'm probably not qualified to answer that question definitively. But let's just stick with breaking and entering as the definition.

Ellsberg didn't break and enter. He was at his office. He walked down the hall. He took something out of the drawer and left. And then he came back. He put things in his briefcase, took them away and copied them with some help from his friends, and then brought them back. He never broke into the Rand Corporation. He was authorized to go there 24 hours a day. And he never entered illegally.

The Watergate defendants, we presume, were not authorized to enter the headquarters of the Democratic National Committee, especially not at 3:00 o'clock in the morning.

Question: Is it your contention there is no such thing as the theft of information? If so, what's the copyright law?

Mr. Ungar: Well, the copyright law is very different. Solicitor General Griswold argued copyright law before the Court of Appeals here and before the Supreme Court during the civil suits over the Pentagon Papers in 1971, quite unsuccessfully.

Copyright law is a very important part of the law, but also we don't have an official secrets act, which Britain has, and we also don't have a Government copyright, which Britain has. You may have heard of things in Great Britain, from which our common law is derived, that there is a Queen's Copyright in Britain and official publications are copyrighted in the name of the Government.

Our Government, I believe, cannot copyright anything. What belongs to the Government, in theory belongs to the people of the country. Individual officers of the Government may copyright their memoirs and what they write, under specific circumstances.

Member: An officer of the Government can copyright his own material under specific limited circumstances. This was taken up, I believe, under the Rickover case several years ago, in which he obtained successfully and it was held up in court his right to copyright an article which he had written on education—not in connection with his own public duty.

Mr. Ungar: That's an important distinction.

The Government cannot copyright, with subsidiary rights and so on, the way a normal copyright works, published information the way individuals can in this country. And I think that's a good thing.

Question: But we still have to worry about protection of information. We can't treat that totally different from anything else.

Mr. Ungar: Can't treat information as totally different from anything else?

Question: Just because it isn't a physical thing, it still may be harmful to take it. Why don't we protect it, copyright it?

Mr. Ungar: Well, we have an Espionage Act that serves us, for better or for worse.

I dropped in at the end of the panel discussion when Bob Maynard was asked which of the various versions he would prefer and he said the existing law.

I think the existing law could be watered down a good deal and still protect information which genuinely needs to be protected in the national interest. I prefer using the term national interest or public interest, rather than national defense or national security, which I think have been grossly distorted.

But the point is—what I'm suggesting is that it is the wrong way and a dangerous way to prosecute somebody for this by prosecuting them for stealing information, the theft of information. I'm suggesting that things like the Espionage Act are adequate to handle the protection of that information. Weapons systems are things that no decent American would want a foreign power to have. And I think those things can be adequately protected under an Espionage Act without charging people with stealing information.

The problem comes, as in any area of law, with the precedents you set. If you convict somebody for stealing information, one administration may be very reasonable and not extend that precedent; but two administrations later someone may come along and use that conviction as an opportunity to prosecute somebody for stealing the truth about Watergate.

I suppose by a strict and absolute definition one might say that information about Watergate was stolen. But I don't think anybody really believes that was stolen. I think we believe that the people had a right to know what was going on and that it went beyond the bounds of what can reasonably be kept within the confidential circles of the Government.

Question: I'm merely worried about your interpretations, going too far the other way, that is to affect people's privacy without the respect to intent but their privacy of information which they have with respect to their medical records or anything else.

Mr. Ungar: Well, with respect to medical records, I think that's a good point. Questions of personal privacy are very important. I think many people in the press—although they have been accused of invading people's privacy and have invaded people's privacy from time to time, and wrongly so I think—I think that if anything the threat to personal privacy and the threat to medical records right now does not come from the press. It comes from people inside the Government like in the FBI. I need only cite the burglary of Dr. Fielding's office in Los Angeles. The motive was not to protect the medical records of Daniel Ellsberg.

Question: But if your interpretation that the Government has no right to protect the information that it somehow obtains, then we have a very difficult situation.

Mr. Ungar: I didn't say that. I said the Government does have a right to protect information which genuinely must be protected for good reason. But what I am saying is that the means for protecting that information—there are very different means and those differences are quite important. And to suggest that somebody can steal information, in the strictest sense, is a dangerous precedent to set. I think there are other ways of protecting it.

I think, for example—I'm very glad you raised the question of medical records and things like that. I think that one of the greatest current threats to the privacy of Americans is something called the National Crime Information Center which is run by the FBI. It has very laudable goals. I mean, I think it's great and important that if a car is stolen or if there's a gun that is illegally transported in interstate commerce, it's very important that the police be able to find out quickly that that car was stolen or that that gun was illegally taken across state lines. But the problem is that the National Crime Information Center is just loaded to the gills with all sorts of uncorroborated information, with arrest records that may not have resulted in convictions, and people's lives and opportunities for employment are permanently damaged by this information being distributed and disseminated without the opportunity for the person to correct the record on medical records, criminal histories. Someone who made a mistake at the age of 20 in something, say as minor shoplifting may, at the age of 45, find himself unable to get a Government job because of information in the National Crime Information Center.

I think that would be a subject worthy of a great deal more attention, worthy of some very severe and strict safeguards on the dissemination of that information to people within the Government, to private employers, to the press, to anyone. I don't think FBI files that are full of rumors and unsubstantiated allegations should be open to the public. I don't think they should at all.

Question: That's what most of their files are.

Mr. Ungar: Then it's time to reexamine the work of the FBI. If most of their files are just rumors and—

Question: They investigate. It's rumor and fact. That's the reason they have a 75-year classification of it. And you find this ridiculous.

Mr. Ungar: What I'm saying is that rumor and fact can be separated from each other. The investigatory process that the FBI follows in a particular case is often very legitimately something that should be in the public domain, after a relatively short period of time—perhaps eight years, perhaps ten years; it depends on the case.

But wouldn't you like to know now, for example, what really happened, what the truth of the matter is in some cases going back over the years that are much closer to the present time than 75 years ago? And don't you think you are entitled to know some of that?

Question: Not when it deals with people, no.

Mr. Ungar: Well—

Question: Not as long as there's possibility of their being alive.

Investigation is not conducted in a simple matter of validating this fact or not. They develop the whole case. They interview this person, that person, and so on, like that; and all of it becomes a part of the investigative record, some true and some not.

Mr. Ungar: Under current standards the way things work now, a lot of people get access on the spot to that information, including people at the White House, people

on Capitol Hill, who just by virtue of a position get access to some of that information and use it against their political opponents, for not the noblest of motives.

I think if there's to be a standard which says absolutely no disclosure of this information, then we've really got to insulate the FBI from a lot of the people who now have access to those files.

Question: That's like saying let's insulate the medical records from the doctors.

Mr. Ungar: I don't think that's the same thing.

Question: Well, medical records are created for medical treatment, for the doctor to treat the patient. An investigative file is developed so that someone in a position with the responsibility can make a determination on that individual.

Mr. Ungar: Well, I think that FBI investigations, except for investigations, for example, aimed toward employment in Government or something like that—I think that most FBI investigations are actually geared for the prosecution of crime—

Question: Right.

Mr. Ungar: —and to be made available to prosecutors. And I would say, for example, that certainly at the conclusion of criminal cases that the FBI files in a particular case perhaps could be legitimately made available to the defendants. There may be exceptions where people may have to be protected because their lives might be in danger, having been witnesses or having cooperated with the Government. But if one side in a criminal case, for the sake of argument—I haven't explored this question in depth, but, for the sake of argument, if one side in a criminal case gets to look at the FBI file, why shouldn't the other?

Question: Are you going to release your sources after you publish your story?

Mr. Ungar: After a certain period of time I think the sources of some information in the press could become public, and invariably very often does become public. I think the ability to protect sources while reporting an ongoing thing is very important, but I think that after a period of time there would be nothing wrong with knowing, for example, how the *New York Times* found out about the Bay of Pigs invasion. And maybe enough time has passed for that. It may turn out that some very public spirited individuals who were worried about the country committing a terrible mistake made that information available and may be heroes when we find out who they are.

Question: Or they may be shot.

Mr. Ungar: I think that probably in some instances like that, the source would perhaps have to be consulted before revealing them.

Are there any other questions or comments?

Question: I disagree with you when you say that the sole purpose of an FBI investigation is conducted for the purpose of prosecuting someone.

In the case of security investigations conducted by the Bureau of persons to occupy positions of trust.

Mr. Ungar: I made that exception. I understand that and I think obviously that's a function of the FBI that it has to continue to perform. I was talking about criminal investigations by the FBI. ■

COMPUTERS AND AUTOMATED CLASSIFICATION—1980

Dr. Lawrence G. Roberts,
Director, Advanced Information Systems
Advanced Research Projects Agency, DoD

I think to address the question which was put to me about classification, I really have to spend most of my time on technology and where the business of handling information will be by 1980. Then at the end I can address the question of what might be done to assist in the classification of that information.

Last summer Dr. Lukasik from our staff gave you a talk indicating that, in fact, information handling would be considerably different, the preparation and handling of information, documents, whatever. And I would like to indicate some of the technology that has already occurred and what is occurring in terms of making that come about.

In fact since he gave his talk I have found all the indications of the need for service which have recently come into existence since his talk, and that is one of a message service that takes care of a lot of the points which he was talking about—the difference between voice and written material. I'll get to that later on in my talk. Also I'm trying to identify how our handling of facts and messages is going to affect the handling of information as well.

To begin with, however, I need to discuss the ARPA network technology which is really changing the base of what we see computer resources around the country to be.

This base is not becoming the computer in your own laboratory or in your own building but is all the computers in the country which may be brought to bear on the particular problem and all linked together.

The ARPA network is based on packet communication technology which is a fairly distinct offshoot of communication technology, considerably distinct from what we have been accustomed to over the past hundred years in regard to generalized communication technology.

Channels were created because of the fact very infrequent decisions had to be made as to the allocation of resources. And decisions, of course, are something that people always have had to make. With regard to the equipment to make those decisions, computers were extremely expensive and not even existent a hundred years ago.

Thus, telephone, radio, and almost all of the original communication media were based on prethought decisions—operators plugging in a telephone channel or radio allocators for radio.

In the last ten years that situation has changed dramatically. Although there was some attempt in the telegraph and its descendents in the earlier period to try to achieve more of a packet-oriented address message capability, it wasn't until the more recent technology became available that it was really possible to make a cost-effective packet communications system where the resources are allocated dynamically by the computers in the communication system rather than by the prethought decision.

This changes the cost pattern tremendously. I think that the important fact for this group is that it now becomes possible with this technology to communicate on a very much lower cost basis between computers all over the world and between people and computers and thus not be dependent on geographic location at all with respect to where the information is stored or initiated. (Figure 1)

I say that because in fact we believe the cost of communication is under 10 percent of the computing cost for almost any application today with this kind of technology. And that means that a very slight difference in the computing cost by optimizing it—by getting it on another computer, by combining two computer centers—can make all the difference in cost effectiveness and wipe out any communication cost, which is under 10 percent.

Now, looking at what ARPA has done about this, in 1969 we built the first message processor, which is something like one-half of equipment. This has been installed at every site within a nationwide network. (Figure 2)

That was the first processor you saw. At later times we had two other versions, a smaller version, more compact, at less cost, and a more expensive version that will handle terminals and terminal equipment as well, so that at any point you don't need to have a computer. You may have a small one like the one you saw previously but one into which you can plug all your terminal equipment to play records, cartridges, tape equipment, whatever you need for communication with the data processing to your people.

Now, in some of the nodes of this network there are those processors that handle just terminals; those are called TIPs, terminal interface processors. And at some locations there are major machine computers. There are approximately 57 computers in the network which are attached to the 36 nodes. These major machines serve as processing capability which people get at through either local connections or in many cases through TIPs.

For instance, in our office building the TIP provides our total communication with processors all over the country. We now have between 40 and 50 consoles in the building, all connected to this TIP. We do all of our data processing through the network to some computer or other throughout the country. (Figure 3)

One of those computers happens to be a small one in our building but a lot of the capability is now achieved through computers on the West Coast or at other locations.

These computers are at basically research sites, not largely production sites at this point, although that's rapidly changing. As of a year or so ago the network was extended to other Government agencies and the rest of DoD as a service which they in fact utilized for putting their own nodes on the network. And as you might be able to read on the slide, Aberdeen and Belvoir are two Army nodes that have gotten on the network. There are several Air Force nodes going on the network, two already have done so.

There is a considerable number of both defense and non-defense computer locations or non-computer locations where access capability to share resources around the country is desired. There's also a link to Hawaii, and recently we included a link to Europe which is not shown on the map, tying in Norway and England. This will be extended with the new technology development for satellite communications to the whole world. At the moment

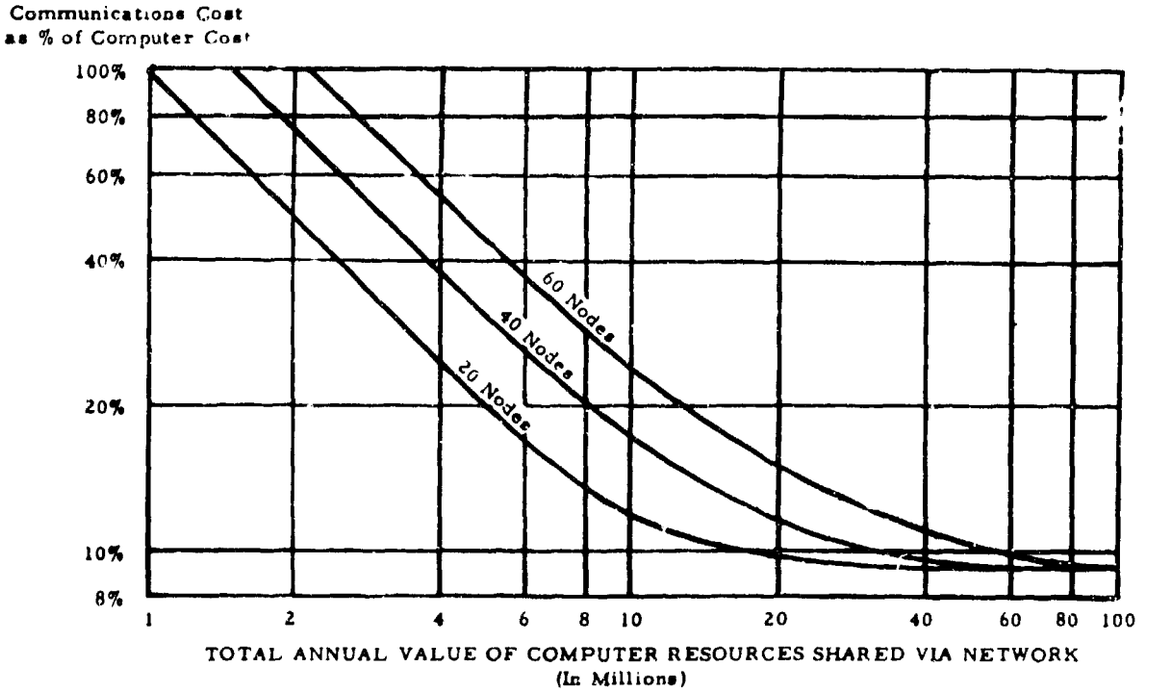


FIG. 1: COST-EFFECTIVENESS OF NATIONWIDE NETWORKS

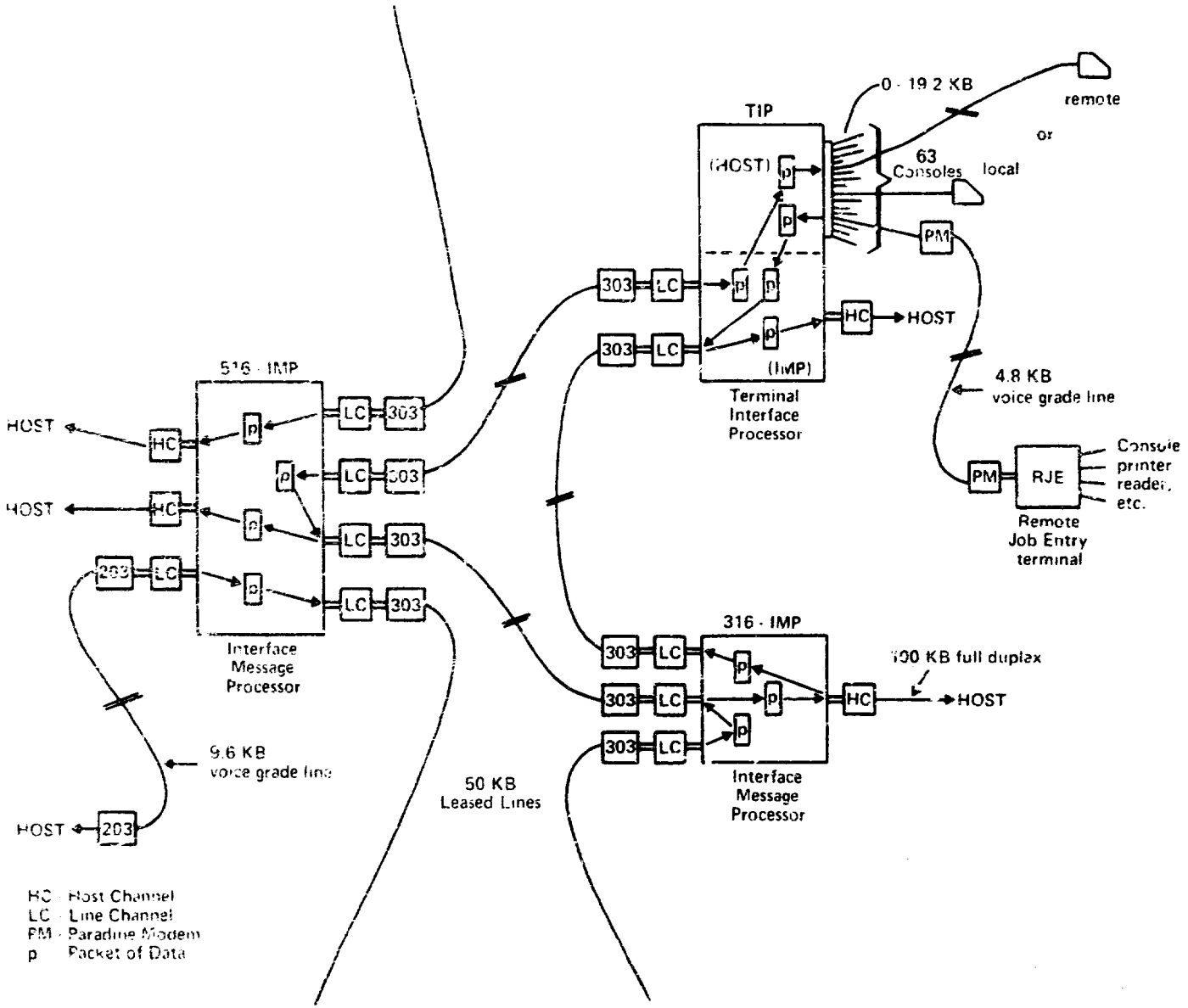


FIG. 2: ARPA NETWORK

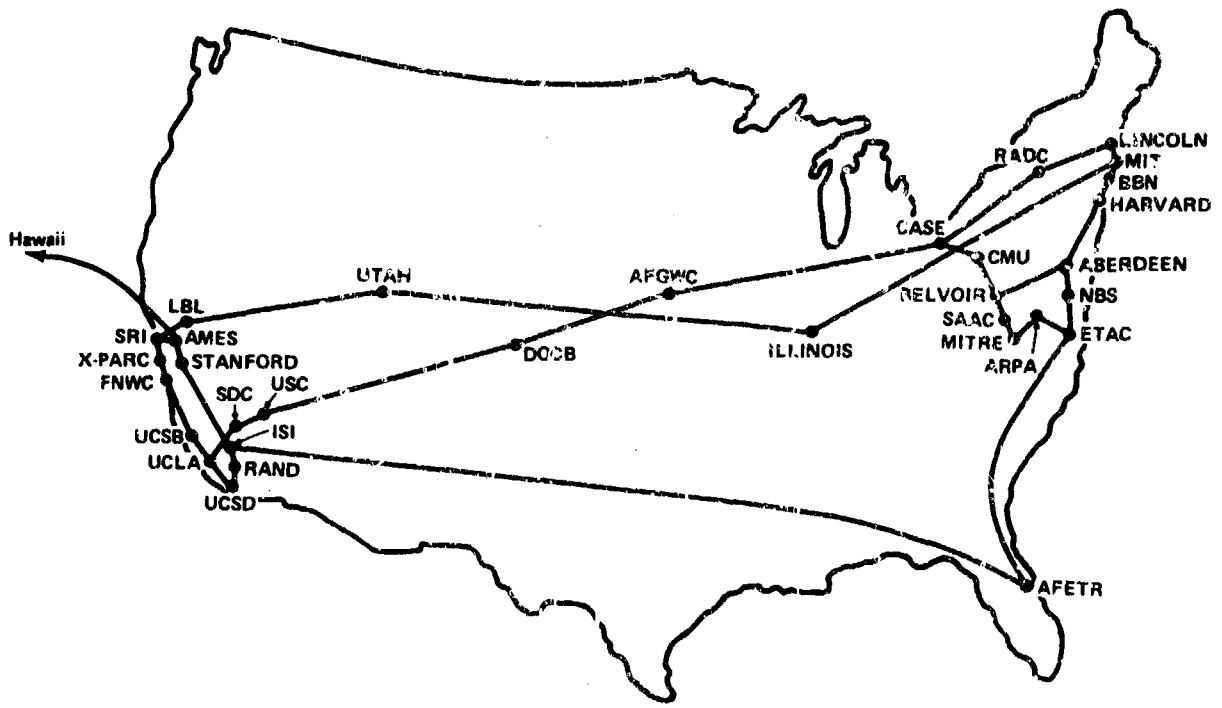


FIG. 3: THE ARPA NETWORK
February 1973

it's just including Hawaii and Europe. But it now appears that the cost of tying in most any place in the world is not much different than the cost within the United States. We'll get to that kind of cost later on. It's extremely low, something on the order of three-hundredths to a tenth of a cent for sending a message to any other location from any place.

To show you what kind of use goes on within this network—this chart is really prepared in terms of our own look at how these resources are utilized and how much money is now being cross-utilized between these locations. But these are user locations doing various pieces of work, and the totals at the bottom show that we're spending something like $2 million a year on computer capability that's being used at a different location in the network than the local installation. (Table 1)

To replace that locally would cost something like $6 million, a 3 to 1 ratio. And that's important, that in fact by doing this, by providing this communication capability which has the response and reliability, you can move computing from any place to any other place. It is usually possible to save on the order of a factor of 3 in the computing cost by now being able to use the right computer for the right chore rather than having to buy a 4-choice computer in your own location, one that is not the best economy of scale, one that is not the best for every job in your location. Normally there are many different kinds of jobs—time sharing patch, statistics—each one requiring a different computer and it's most cost effective on the *right* computer.

These computers are around the country and if they can be accessed at sufficiently low cost with sufficient response and with capability, then there is no need to try to duplicate that resource locally. (Table 2)

So if I want to look at just one of those, the top case, for example, the University of Illinois is doing research on data processing. They in fact were the originators of the ILLIAC-IV computer concept and went through a large phase of development with that computer. The computer was eventually installed at the University of California.

The University of Illinois people still work with that computer and work on programming it. And in order to do that they need a large secondary computer, a B-6700, to do their program preparation. That computer was located at the University of Illinois, but as the network developed we were able to completely eliminate the need for that machine and replace it with access to one in San Diego which considerably reduced the cost. Now we are able to share a larger complex and just buy a piece of that machine rather than paying for an entire installation.

Secondly, they need access to the ILLIAC itself at NASA. A considerable amount of the computation was done there at this point. There may be access to several other time-shared machines in the network for doing editing and other programming work, and these are accessed at several other locations in Boston and L.A.

The entire computing complex would have cost them, if we did not have the network, something like $1.1 million and they still wouldn't have had access to the ILLIAC, whereas it's now running something like $360 thousand, a saving of in their case something over $530 thousand. This is quite typical of the kind of cost saving we are achieving within the network.

That gives you perhaps a rationale for its existence. It

TABLE 1

REMOTE USAGE OF COMPUTER SERVICES WITHIN ARPANET
Annual Remote Computer Usage Cost Based on March 1973 Data

Service Resource	Computer	Remote Usage ($ in thousands)
Univ of Southern Calif, Los Angeles, Calif	PDP-10	520
Inst for Adv Computation, NASA-Ames, Calif	ILLIAC IV, PDP-10, B-6700	470
Univ of California, Los Angeles, Calif	360/91	340
Bolt Beranek & Newmen, Cambridge, Mass	PDP-10	179
Stanford Research Institute, Menlo Park, Calif	PDP-10	151
Univ of California, San Diego, Calif	B-6700	118
Mass Institute of Technology, Cambridge, Mass	Multics-645	90
Others	Mainly PDP-10s	150
Total		2018

TABLE 2

COMPUTER RESOURCE USAGE WITHIN ARPANET
Annual Remote Computer Usage Cost Based on March 1973 Data

User Organization	Activity	Remote Usage ($ in thousands)	Projected Cost for Local Replacement
University of Illinois	Parallel processing research	360	1100
NASA Ames	Air foil design and ILLIAC	328	570
Rand Corporation	Numerical climate modelling	210	650
Applied Data Research	ILLIAC IV compiler development	151	470
Lawrence Livermore Lab	Dev of TENSOR code on ILLIAC	94	370
Stanford University	Artificial intelligence research	91	180
Rome Air Dev Center	Text manipulation and resource evaluation	81	450
ARPA	On-line management	77	370
Seismic Array Analysis Center	Seismic data processing	76	300
Mitre Corporation	Distributed file network research	60	240
National Bureau of Standards	Network research	58	200
Bolt Beranek & Newman	TENEX system support	55	80
Xerox Parc	Computer science research	47	100
USC-IPL	Picture processing research	35	70
UCLA	Network measurement	28	90
Systems Control, Inc.	Signal processing research	23	70
UCSB	Network research	22	70
Range Measurements Lab	ARPANET management	17	60
Institute for the Future	Teleconferencing research	13	40
Miscellaneous	Computer research	192	580
	Total	2018	6060

doesn't say what it does in the case I'm talking about here. It just gives you some feeling for the economics and reason for the network's existence. (Figure 4)

Due to that and due to the cost economies involved, we have seen the traffic growth in the network from 1971 until more recently, over the past 15 to 18 months, of a factor of about 26 percent per month increase in the traffic on the network and in fact in the computing that people are doing through the network. It is now something like 2½ million packets per day, each packet being a line or two of text; something up to 1,000 bits of information if you want a precise definition, and the network capacity is somewhat beyond that but we're rapidly approaching the top of the graph which is in fact the current capacity of the network. That can easily be expanded, but it will be when we reach that point.

That just gives you some idea of what's happening within the network, that traffic in the network is closely related to the computer activity within the network with all the activity of computer usage. And all of that is just indicative of the fact that this kind of network is cost effective in itself and will permit computers to be used wherever they are rather than being a local installation.

Now, what about security within the net? Clearly if

we're going to talk about classification we also have to talk about the questions of classified and unclassified computing activities and working with classified information on these computers.

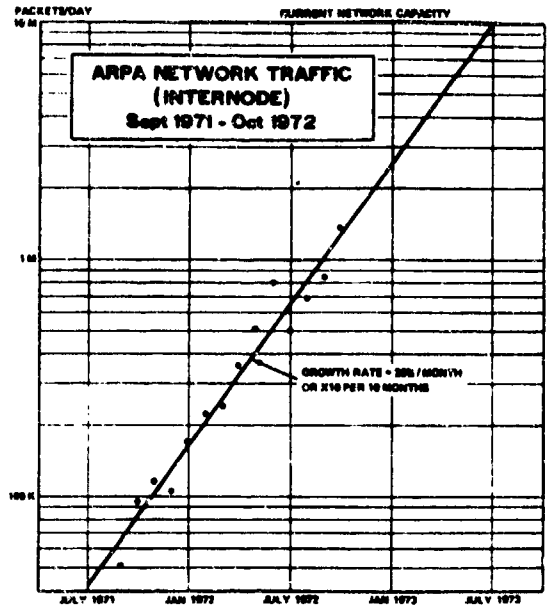


FIG. 4

ARPA has for a long time been involved in a number of aspects of this. One is with respect to the network. We have been working on the task of permitting classified information to be used within the network. It is entirely an unclassified network as it currently stands but in the near months we will be installing equipment to permit end-to-end communication through the network on a restrictive basis so that in fact people at one location can use machines at several other locations, all of which are totally secured, and the other people on the net don't have any way of getting involved in this process because of the fact the packs of information themselves are encrypted. This is just following fairly standard computer practice except we don't encrypt everything. We don't secure the whole net.

There is another possible avenue for a totally secure net but in fact my main point is that end-to-end security is quite feasible, quite inexpensive, and something which is very close to being actual fact within the network.

Thus if there is a secure computer one is operating at one location in the net, it is completely feasible for a TIP at another location in the network (perhaps across the country or perhaps even in a different country) to have full access to that computer and its capability. And all of the consoles, printers, and other equipment attached to it, are working through this one network task and don't each need their own system and everything like that.

I should mention something about the characteristics of the network in terms of required response, the sort of thing that makes this all possible. The network will deliver a packet of information to any other place in the country within a tenth of a second and will move a continuous flow of information, say a file that you're moving like a tape, at rates which are like 30 kilobits per second which is a quite reasonable communication rate. That means you can move a full magnetic tape in 40 minutes anywhere within the net and people in fact find this quite effective for moving tape largely due to the reliability.

The error rate in the network is one or less undetected error or transmission error per year, a rate like 1 in a trillion. The main problem, if there is one, within the net is reliability. At the moment the network reliability due to the redundancy of multiple lines and everything else is something like 98 to 99 percent. We are trying to improve this through improving the message processing you saw. If reliability falls below 95 percent you have a serious problem for the user, but at 98 or 99 it does not appear to be a major problem. However, for some jobs it becomes serious.

Now, what about security in the operating systems and the computers themselves? If we can have the network handle classified data between locations, we now still have to have completely independent machines for each classification of material and that involves an awful lot of security problems. So you get into tasks that I have been working on for several years and one in which I think progress is being made, although that may not be apparent. Regulations have changed. In fact, it is now permissible to run a machine at a local level, if you can get approval. Approval is rather difficult to come by It hasn't been granted yet to anyone, but at least one is permitted to strive to get it.

We had a project attempting to provide technical advice for the certifiability and the penetrability of operating systems, to try and analyze the security behavior of computer systems and particularly the software involved to see if in fact it can be certified for multilevel operation. This project has now been in existence over a year and has developed a considerable body of experience on what the problems are in operating systems, how to penetrate them, and how to (in fact) fix them so they can't be penetrated. They are working together closely with a number of manufacturers to try to improve the security of various operating systems to the point where some of those will be accepted.

It is my current belief that within the next year a couple of operating systems (and these will go by types); in other words, a particular operating system will probably be much easier to clear than another—a couple of types of operating systems may be cleared in the next year, because they have, in fact, been well designed for security in the beginning. Other operating systems, which were not designed for security in their first implementation, will perhaps never be certified. They may need to be redone by the manufacturers in their next round—or the manufacturers might find ways to fix them up. This is being pursued with a number of manufacturers so that some of the older systems, where security was not a particular concern when they were being built, can be improved. But you can imagine the number of mistakes that can be made in a system where you had no concept of security when you built it. You'll find millions of such mistakes in some of these systems—thousands at least have been documented.

And these mistakes are very hard to detect. We've gone back over some of these systems and the ratio of effort is tremendous. We have to spend a certain amount of effort to point out flaws. So it does require a fairly good system before the person who wants to break and enter that operating system could break in and take control of it or gain access to information through that. You can't do that with relative ease.

In fact, we don't believe there is any system today operating which is secure in that sense, at least in the commercial world, and against, say, a few weeks of effort for penetrating. There are plenty of systems which are fairly secure. In other words, the average user will never get in any other person's data. As a matter of fact we're using some of these with ARPA for protection of our own information which may be private, sensitive, that sort of thing, but not for classified data because there you can see the threat is considerably greater than just a few men making decisions.

That is the main problem, that the penetrator, the person with an intentional desire to take the operating system can in fact take over complete control of the system by taking control of this system. At that point then he has the option of looking at files, destroying them if he wishes—which is one of the threats—denying service to others, and generally doing anything he wants without observation, because at that point he can also cover his own tracks. This is in fact what we have done. We have made penetrations of systems and usually this is not discernible by the feeble operating equipment. That has to be improved in the systems and I believe we're fairly close in several of them to achieving security which we would be quite happy with, so that people could operate in multilevel modes.

At the moment, however, it is certainly possible to have some machines operate at a Secret level and other machines on a classified level totally, and share those through the network. So, at one installation you might have access to several different machines, each operating at a different classification, and thus not run into the trouble where you have to run your machines for 3 hours at one level, 3 hours in another, and 3 hours in still another. People got together and said, okay, we need a total of 360 operating in Secret between the Government agencies here and another operating on Confidential or Top Secret information. The network would permit the shared use of machines by people at a particular installation. At the moment that's our objective—to gain multilevel use of machines.

One point I want to mention is password control and the whole question of access control.

There have been a number of potential improvements here which have not yet been widely implemented but I think will, in fact, improve the situation considerably in the future. One of these is if you think back to the question of breaking operating systems and entering them, the immediate thing that the penetrator will adapt is a whole set of passwords of all the users. Then he has a password for everybody and that's the end of the job. He can then go back and use anybody's password he wants to.

That process of course can be effected by one-time password which the user uses once, but not totally because he could get the whole password list from the machine. And, secondly, it is very hard to protect against, because it only takes a momentary break of the system to get the password. And it's usually stored in an obvious place. It's one of the things the operating system is trying to establish.

So it's something which we certainly want to protect against, and it's more than the actual tapping of communication lines and similar types of physical threats. It's much easier for a person to sit at his computer than it is for him to go out and penetrate the machine physically or penetrate the communication physically.

Thus, we are in fact beginning to institute a password system whereby the password itself is only encrypted once. In other words, the user sends this password to the machine. The machine never stores it, it only transforms it in an irreversible transform and then checks that against the stored transform.

You could publish that transformed list and it wouldn't help him—he still has to find the right word to enter it, the password, before the transformer comes up with the stored word. And there is no way to go backward. This in fact provides a very desirable additional protection that the password list stored in the machine is of no use to anybody except to check legal passwords.

That has another implication. It means that you can also use one password for a number of systems, each one having a different password and have all work without any control system. There are a number of processes like that which are now coming about that would make it quite feasible to have fairly good control over access. We will be quite happy with the process as long as the passwords are changed at rates frequent enough as dictated by the particular level of the system. And that of course may vary depending on the people involved and the tightness of their own use.

Now, there is also one other thing associated with this and that is something that is starting to be used, the signature authority. If a person has verified that he is who he says he is by an appropriate password system that you believe authenticates him (and, of course, we have to design what you believe to be sufficient—one of these processes which we believe to be fairly inviolate). A user has now identified himself as who he says he is then, we can record permanently the fact that he has signed a document, by virtue of that recognition, and store in the file for retention that fact. If, then, a question of authenticity arises, or a copy of the document comes into dispute as to validity, the facts or data can be compared with the record to prove whether the stated individual did sign the document. Verification can be certain because only the properly identified person could have stored anything in the file being queried.

This kind of system can be quite effective. It certainly is as good as the current system.

Next I'd like to talk about a use for all of this which is now coming about. And as I mentioned to begin with, you might have seen the intent of this in Dr. Lukasik's speech last summer, as he described the actual management technique within ARPA and the rest of our community. That is the use of messages and the interchange of small pieces of information in message format between a large number of managers. Here I need to describe the basic problem with voice and messages to try to give you an indication of what the problem was.

A written piece of paper, a document, has wide dissemination ability: you can study it, you can remember it easily; you can control it; dissemination is accurate. Those are properties of a written document. Voice, on the other hand, has usually totally opposite attributes—its interaction rate is higher; you can interact and clarify details; the cost is much lower for the preparation; and there is no permanent record, so you won't be inhibited in saying some things you might be inhibited in saying in written documents.

Those things are not totally separate from each other as they tend to be achieved in the same system. My point is that the message system that we are now using within the computer has all the properties of both. That's achieved essentially by a management decision to change the property of messages from being normally recorded and available for public certification to being normally illegal to record just like voice. That's the legal distinction between voice and written copy rather than a technical distinction. We maintain very private distribution and access control over message transmission. Dr. Lukasik uses it very extensively at this point. For example, his personnel manager can discuss a candidate quite freely without any fear of people subsequently printing these things or violating them.

Secondly, the interaction rate is very high once you're on-line and talking through the computer that we're referring to. Interaction rate is such that a person can send a message and the other person will receive it within an hour or so, maybe a day at the most, but the interaction rate is in fact quite a bit higher than trying to find Dr. Lukasik in his office, which is considerably difficult for a high level defense manager to do.

I'm sure this is true of most high level people, and in fact this is one of the reasons why this service has become extremely effective at the top echelons of the organization rather than at the bottom. It is the first time I've ever seen a high-level manager start to use a console himself in his own office and even at home if he weren't just concerned with computing for some reason for his own management purposes, rather than having a secretary or some staff level person doing it for him. In fact, it's part of his communication process. It's very important and even far superior to calling the other people on the phone, trying to send them messages through secretaries, and so on.

I can't necessarily convince you of anything on this. I think the effect has to be seen. In fact, it is quite striking, much more so than you would imagine. This kind of information transfer for questions, facts, and communication between people—including most everything that would normally accompany a letter and memoranda—is becoming quite extensive. It permits multi-addressed messages. I can send a message to a contractor three levels down from me but encompass all the people who should hear about it in the process plus the other people who are in the same field and need to know about it. All such interactions are handled in complete privacy as well, so that it's only that select group and not a whole collection of people involved.

Then they can copy the message, pass it on to another person who may be an authority to do that and needs to see it. That means that this thing has a permanency to it that permits a person to keep track of it if he wants to in his own private files, but it has the same properties as voice and there is no record of it unless one of the parties makes such. And it permits most all of the properties of written communication.

Now, that kind of use is quite widespread in ARPA and throughout our contracting community. It has proven to be extremely effective. I should mention that one of the most effective places is with overseas offices like Europe and Hawaii. The time difference is such that we can't get information to them any other way. We can't get in touch with them on the phone or anything else right away. So this in fact is making considerable improvement in our ability to communicate with these people.

Why do I bring all that up? I think that's one of the parts of the changing environment that might be vital to know about, perhaps using it in some way. On the other hand I think it's an indication of the first use of small bodies of text—now we're talking about something that a non-typist is preparing with maybe considerable effort but far less effort than getting someone on the phone—but in fact it's short and crisp and to the point and just the communication that needs to be communicated at that point, not a long drawn-out conversation that you usually happen to have on the phone which has many topics covered all at once. These are terse topics that are passed back and forth of action or questions or whatever.

Each one in fact has to be classified separately. Each one has its own audit trail, if you want to create one, and each one is in fact part of the body of knowledge which will be our main written record in the future, our main body of record to be stored in the computer. It can be printed out and saved on paper if that's desirable, but that's probably undesirable. In fact, you can file it under topics, under author, whatever you want, and retain the pieces of information which are appropriate to save within each officer's and person's file.

In fact you can transfer a whole filing system and a whole change from the written kind of communication of the past to an on-line system. In some cases these messages are distributed to hundreds of people and have open distribution. That's an option which in fact you can elect.

Thus, you can conceive of a situation where most of your memoranda, letters, and other longer information are all stored on-line and filed in this kind of way.

Now we get to the question of what might be done about the classification process.

The first thing I'd like to say is that in the consideration of multi-level security, the group which has been involved with it studied the question of the use from an originating point of view, not the classifying. They concluded that there was a certain amount of automatic evaluation of sources possible. It was something which was not complete, something that would not give this generator of material an absolute classification level but something that would give him a guide saying your reference copies of material here, and a composite level where you should be thinking about Top Secret in creating this new document.

And if you're referencing at a low enough level piece by piece and fact by fact and each one is appropriately classified, then this is not too far off as an estimate of classification.

There may have been some new text put into it which may change the classification; or there may have been extracted just some little piece of a classified fact. The final determination is made and it has to be reviewed in any case, either way.

So you have a guide to keep you from making gross mistakes about referencing Top Secret documents and then classified and unclassified without thinking.

It can happen, of course, that you make a mistake and grab a piece of the document without even knowing it. You have to realize the user may never read all the material you prepare (physically read it). He may just grab a little piece of this, a little piece of that, a little piece of that one over there, and put it all together and say there's the document. He may never look at it. In that case there has to be something to indicate that he ought to look at that part.

Now the next part of the question is what about the classification from the user's point of view, in that clearly we can help him. I can't say we're going to do the job for him. That would be, I think, something which would require vastly more computing parts than I'm even going to try to project at this time. But we can, in fact, have the classification guides for him so that he can select from them and create the proper information that he needs. If he needs information on a particular subject and that was a subject which might have been worked on in a weapons lab and they have written a classification guide for it, he could perhaps access that classification guide, under the criteria that he wanted to know about a certain weapons design and information relating to it. That request would be sent to the weapons lab and coming back would be the section or the entire security guide associated with it. Then he could use that for his purpose in classifying which are problems.

Required for that would be the fact that he would put these things on-line and make them retrievable. The technology to do it is not a problem. The thing that has to happen is that the people doing the guide preparation get those on machines rather than on paper and then the rest is fairly straightforward.

The second part of that, however, is so that the person can get some assistance in looking over the documents. Here I have to resort to some of our further out technology. I don't expect it will be available instantly. But there is in existence in our research program quite a bit of expertise now in (English) understanding. In other words, being on tape, almost any English text you want, take it apart, understand the concepts involved, and make essentially decisions or in fact direct action on the basis of the understanding of that text. Let me illustrate that a little bit.

Just looking at a sentence and breaking down the structure so you know where the verb is, is what I mean—that's not even a step in the process until the latter end. The first thing you look at are the important words and think about the phonetics in the program. Then you may look at the syntax of the structure. And finally you come out with a concept which is something like in a sentence "the boy threw the ball," a relationship-threw-between boy and ball. That's the concept. That's the relationship which you extract from the sentence, and now store and utilize. You store it under "boy" and "ball" and "threw" and all of the things that are related. Now as you go through the document you collect all these concepts—this is a program which in fact requires considerable computer power but that won't be terribly expensive in 1985. It would be today.

You could then show to the classifier those sections of text which skip the security guide statement. That would just be a guide in an age. The main thing I could perhaps suggest at this point is that you could filter out and point out the sections which talk about sensitive projects where the concepts involved were related to things which were in the security guide as being classified, and thus put together for him a number of displays and pieces of information which show him both the section of text and a relative guide quotation so he could make a determination. This would just speed up his process, not completely eliminate it.

And that's about as far as I think we might get in 1980. Something else may happen in 1990.

Questions and Discussion

Question: If I may propose the first question: Do you think it's potentially feasible that by 1980 we could have on-line files of classification guides available to all of us in our respective across-the-country locations?

Dr. Roberts: I'd say that's feasible, extremely so, as long as the decision was made at some joint level to do that, including the individual level, that one group intended to do that. But it wouldn't be terribly useful until all the relative material was available.

Currently there are a large number of research installations on the network in the Government activities. There will be more and more of them in the near future, and any which wanted to participate could get console access or other access to the network fairly quickly. There are many locations in Washington you could tie to. Similarly, you might want to tie your own computer in.

So, if you set this information base off on one of the stores that we are now installing, and we're installing two, one on the East Coast, one on the West Coast, so that we have very large stores, 12th depth, which is able to be retrieved on a context basis.

In other words, if you have stored information there on a certain subject, you can retrieve it later on by context or by whatever it's filed under. Then in fact working with one of the other computers in the network which do the initial text editing and text handling, you could have both the processing and storage capability to do the job economically today. It is economic.

The cost for storing a document today might be $1 a page a month on a standard machine, whereas in the large store we can bring that cost down very considerably to where it's like $1 a year a book sort of thing. So we have a considerable change in terms of the storage cost.

The processing cost, we're already in the right ballpark. The on-line method is probably cheaper for an author to use on the computer today to aid in text preparation than to have a secretary retype it a number of times. So that's already in the ballpark of being very reasonable. This is so in communication if you get at it.

So we're talking about something that's just a management decision at this point. And I expect if you look at

that as the normal course of events, that might still be five years before somebody decided to do that. It could be six months. It's all a question of how important it is and how much would be achieved by doing that.

Question: In the early part of your presentation you were discussing the transmission between computers of classified information. I believe that's what I heard you say.

Dr. Roberts: Transmit it, yes.

Question: I presume then that you are using crypto machines obtained from NSA.

Dr. Roberts: That's right, but in a special way.

Question: What special way?

Dr. Roberts: Well, they're used in a somewhat different way than normally. In other words, they're used—as a matter of fact the whole process is approved and is standard, but they are only encrypting, say, a thousand crypts at a time, a piece of information and not a whole stream.

Question: Are your codes controlled by NSA?

Dr. Roberts: Yes, the whole process is under their control. It's just using that equipment in a way which makes it possible to use it in two different points in the net.

Question: Do you foresee in your planning approval of commercial crypto equipment for contractors to classified information?

Dr. Roberts: Well, there is a distinction of whether in fact it's for commercial purposes or for DoD purposes, and I can't tell you what the entire approval chain is for contractors getting hold of crypto equipment. If it in fact is sponsored by a Government agency, if they want them to be working with that information, sure, we are doing that. We're putting equipment in locations under Government control, under the appropriate security measures. That involves contractors in some cases.

However, for your own purposes, and maybe it's incidental that that includes classified information, there may be a different case. Clearly in the purely commercial cases where they are protecting their own secrets and their own information, a device is needed of a commercial type which is both secure and approved. I mean it's not classified. That is something which is feasible today but something which is not widely available—something which may take some policy to let it occur somewhere.

Question: Then if in talking now about a dedicated system in your facility with no external access. You fix your system so that one can have access when you're handling a classified run. In your remarks, did you say that you expect to have two systems approved very soon for time-shared operation?

Dr. Roberts: That's on a multi-level basis. I think there are two operating systems. The Multics system which was built at MIT but is now being marketed by Honeywell, which has appropriate security provisions within it to make it feasible to certify. I'm not saying it has been certified but it's very close. And, possibly the Tenex system. Now that's hypothesis at this point until we actually prove that. Those systems to our way of thinking are the closest to having the right security controls in them to being with, Multics probably being the best.

Question: What was the second one, I'm sorry?

Dr. Roberts: The Tenex operating system built by Bolt Beranek and Newman. The Digital Equipment Corporation is now making that available. It is another operating system similar to Multics in terms of general structure.

The hardware has very considerable hardware protection capability, particularly in the Honeywell case. The new Honeywell machine that supports Multics provides several rings of protection of different levels. In the inner ring you can get at everything, at the next ring you can get at only some things, and so on. That's hardware protection, and the software has to utilize that properly which it was designed to do.

In the Tenex system there are only two levels of protection, user and executive, like in most computers. Many computers have that kind of hardware capability, but it has to be properly designed into the operating system which is the real question involved, and that it's used properly.

That has to be done almost from the start. If it's done from the start, the cost is very low. We feel that the cost is not much more than a system without security if the concepts are kept in mind from the beginning.

But if it was not, then we very commonly find people putting code in the user area under user protection rather than executive protection, which is needed for executive operations. If you compromise it, it compromises the system—and many other such things—which were not intended but they ran out of space and used some other space. They didn't pay much attention to that fact.

So the fact the machine has a hardware protection depth, the actual protection of hardware that separates the executive from the user, does not guarantee anything. Then, of course, rebuilding these systems to make sure that these things are not done, and a lot of other possible flaws, is necessary.

One type of system can probably be approved very much more rapidly than all this. That's the system where in fact no program is involved, a pure retrieval system where the only thing you can do is give a standard request and get back standard answers. It retrieves from the file. But it does not allow you to write a program or procedure.

In those cases the restrictions of the user are so much greater. He doesn't have the flexibility of writing his own program and doing his own thing in the machine. There is no way for him to penetrate the machine with the same ease that he could otherwise. None of those types of systems has been brought up for serious trial at this point but I think that would be a possibility.

Question: Who do we come to for this type of a trial or certification?

Dr. Roberts: Actually the people to go to are through the appropriate channels—the office we work with that finally gets the request is the Office of the Secretary of Defense, Security Policy. They then reflect with us on whether the proposal in fact merits our looking at it—or someone else's—or what the process should be.

In some cases where the need is high we have in fact reacted to contractors' requests through this route and helped with work with their systems. In other cases that's not feasible since this is an R&D program to develop the technique. Next year we hope to turn that process over

to the Security Policy Office as more of an operational process, which they then would manage. But at this point we're hopefully taking the best route to developing the techniques with the systems we think most profitable and actually working with four or five different systems to try to develop a capability. Now, in fact, there are almost separate entries being done in the GECOS system and that's being done by the people involved to try and certify it.

The only thing that really needs to be done is to get security policy approval with the contractors, GSA, the appropriate officials' approval. That can be done by any proof but the proof has to be sufficient, and that's where we're involved. ■

INSIGHT INTO THE BELL SYSTEM PLANS FOR 1980 AND BEYOND

Mr. Charles P. Buckley,
Manager, Comptrollers Operations
American Telephone and Telegraph Company

In talking about the effects of automation and computers in the Bell System, I believe it is impossible to appreciate what it means without thinking in terms of the future. But, the future must be considered in the light of past effects of social and technological movements in the history of the world.

Let me explain. One lesson which study of the history of technology drives home to me with great force, is the essential unpredictability of those secondary effects which technological developments have on the social structure of society, business, and government.

To illustrate, an author and journalist, with long experience in the Middle East was asked recently: "What has happened to the Arabs? In the last thousand years we've heard little from them even though they once led the civilizations of the world. Suddenly, however, in the last 15 or 20 years, we see great things happening. They seem to have found a sense of destiny, nationhood, and unity. They are creating a great deal of activity with which we are uncomfortably familiar. What's happened? What caused this? What factors are at work?" The journalist replied that the availability of the Japanese *transistor radio* was a very influential factor! He went on to explain that every camel driver, every oasis, every little village, now had Japanese transistor radios that are tuned to the "Voice of the Arabs," the characteristic name for radio Cairo. Incidentally, it operates 24 hours a day and is the largest broadcasting complex outside Russia or China. These widely scattered people—many illiterate—are suddenly able to receive a message in their own tongue that calls them to power and glory. They listen and act.

Now, let's go back to 1948 and imagine that you are wandering through the halls of Bell Laboratories at Murray Hill, and you come across three shirt-sleeved individuals. You ask, "What are you working on?" They reply, "You're in luck today because we've just invented the transistor." I believe that if you had casually observed, "That's wonderful; won't that be a great boon to the unity of the Arab world?" probably they would have looked at you in some amazement—if they did't call the guards!

Yet, this is a problem that faces anyone discussing the impact of technology, such as the trends in the apparatus of automation, on society or our business. All we can do is point out some of the impact of these forces that together with political, cultural, and economic forces determine the shape of our nation, its society, and our business for the future. I can't exactly predict when or what will happen, but here I will use the "other-things-equal" approach, and point out the kind of developments one might reasonably expect.

Consider another example. In the case of Martin Luther there isn't one item in the theses that Luther hammered into the door of the cathedral in Wittenberg, that was not known previously for centuries, or had not been stated by "heretics" ranging from Huss, Wyclif and all of the others known now only to specialists.

What made Luther different? From the narrow point of view of technology, he enunciated and hammered these heresies on the door at the very time that printing was coming of age. It had only been in the European world a short time when he brought forth his thunderous message. His virile prose, carried by the invention of printing, altered world history. Had you gone to Gutenberg and asked, "What effect do you think print will have on Europe?" he might have replied, "I'm interested in getting out some books." Just as today, if you ask some accounting people "What effect will computers have?" they might tell you, "I'm interested in getting out some telephone bills. We could multiply these examples interminably, but the only important point is that no one can predict precisely what the organizational and social implications of a particular change will be. One thing I think we can say is that predications found in trade journals every now and then—the "Gee Whiz" school of projection—are often sterile because they merely say that this invention or that particular piece of technique will mean that everything we are doing now will be done faster and in greater quantity.

These projections are of the kind you might have expected from a foreman on the pyramids of Egypt as you showed him a power crane. You might have asked, "Tell me, sir, what effect do you think this power crane will have on the Egyptian society?" And, being highly sophisticated in mechanical devices he would reply, "Obviously what we can expect is that we will be able to build pyramids much higher and faster, and perhaps every Egyptian will be able to have a pyramid of his own." We know, of course, that this isn't the kind of thing that we are projecting. We often see projections of technical inventions which are short-sighted and do not take into account all the possible ramifications, but it is necessary for us to sense some of the changes in response of the society and of our business.

One way to look at the history of political, social or buinsess organizations is that their evolution has been influenced to a great extent by the control systems available to them. We can, of course, look at these from several points of view—economic, military, social, and so on. But here let's think in terms of the developments in world history as responses to the control systems which were available. In prehistoric times, the cave men had to

operate in essentially a "real-time" operation. There was no time to store food; things had to be done quickly as problems presented themselves. This approach, where the response to conditions takes place immediately, is really the natural mode for human beings—this is the way most of us operate every day in our own work.

In the formation of the Greek City-States, the area of development of any particular City-State seems related to how far a man could go in a two-day journey; one day out and one day back. Almost none of the Greek City-States developed a geographical size larger than a two-day journey. This suggests that the time for decisions and problems—the delay one could tolerate in arriving at decisions—was limited by the communications system. It was also limited greatly by the diversity among the City-States, with no general agreement on what the desired goals of society were.

In the case of Rome, we see decentralization, only because certain technical inventions permitted the administration of a much larger area. The first of these was the legal system which is similar to our body of operating practices. These practices allow us to have a decentralized operation with uniform application. The Roman system of law was a great technical invention, and was coupled with the use of disciplined armies and the building of superb roads that allowed information, including descriptions of major problems, to be sent back to the capitol for timely, yet far-reaching, decisions. This system overextended itself and, in its collapse, centralized decisions could not be maintained partly because the roads were destroyed by the barbarians, and the armies could not enforce the uniform legal code.

Think in terms of this, if you will, that capitalism was feasible only after we had the technical inventions of money and credit, a great deal of literacy, and in my own particular area, the invention of double entry bookkeeping. It is impossible to imagine capitalism and the building of modern nations without these controls and organization, the record keeping so essential to private property, and so on. So much, then, for this rapid excursion into control systems.

What has been the pattern of this history? It is one of growth to larger units over many years, but the growth is always limited to the control system of communication, awareness, and decision that has been available.

What do we mean by control? Control is a tricky word in English because from one point of view it means the control of crime, disease, behavior—i.e., restraint. But, control also has the meaning of controlling an airplane, car or battle. When we use the term control in "management control system," we mean a timely adjustment of forces inside a business to unforeseen or impossible-to-plan-for changes in order to achieve a goal. It is not a constraint, but an adjustment to circumstances as they change an operating environment.

Now, what is the management ideal that we would like to attain? I think it is total corporate involvement to give our customers the best possible service from initial demand through final supply, in the shortest possible time with the minimum required resources. One of the best illustrations of this appears in the autobiography of Benvenuto Cellini where he describes the casting of his great statue *Perseus*. This story is worthwhile reading because it illustrates what personal management, motivation, and involvement can really accomplish under critical conditions of time and effort.

Cellini secured the funds, set up the shop, hired the men, and started something which all contemporary experts said was impossible. In the midst of his trials, they prepared for the casting. As he starts a furnace of his own design to melt the bronze, the shop catches on fire. He then has to supervise the fire fighting. Just as the fire is put under control, heavy rain pours into the shop and he suffers severe chills, and has to go to bed. While in bed with a fever, he gets frantic messages from his men that the molten bronze is caking up the furnace and that the entire project will be completely ruined. He dashes from bed shouting instructions at his force. He arrives on the scene and throws in hundreds of pewter pots and dishes from the neighborhood, commandeers everyone's wood, and rekindles a roaring fire to the accompaniment of the cheers of his men. Just as the caking is reduced from the metal, the furnace explodes. At that point he sends everyone outside to pray! In the midst of the confusion the men scratch a ditch in the floor which conducts the metal from the exploding furnace into the mold which rests in a large pit. They do this successfully, and we have as a result the great statue standing serenely in Florence today.

I think the anecdote illustrates the objective that total involvement of managers comes from a sense of the actual things they were accomplishing, contrasted to the vicarious world of reports—should this not always be in our mind in dealing with motivation?

Today computers—the present generation of computers—allow this kind of involvement in the operation of a business on a large scale. This is a significant fact for us today, together with the awareness that present machines possibly allow a rehumanizing of work in the future as contrasted to past mechanization systems.*

If history is a prologue to the future, what can we learn and apply to today and tomorrow's world? A few points suggest themselves.

- Computers must not be elevated to the level of an omnipotent being—where only a chosen few control our destiny
- Secondary effects of their widespread use are largely unknown
- Understandable controls, standards, and procedures are a prerequisite if wider participation in the computer technology is to be realized.

Fortunately, we see the computer industry changing—giving the users a broader spectrum to choose from, all the way from super powerful processors to economy-sized machines.

High level programming languages such as Cobol and Fortran are becoming more and more efficient and, as a consequence, allow wider participation in program development.

We in the Bell System are placing more and more small computers in the hands of our operations managers in all phases of the telephone business. They are used as diagnostic aids, communication devices, and record retrieval

*Boettinger, H. M., *Some Reflections on Computers and History*, AT&T, New York, N.Y.

systems. Until very recently, the Bell System had centralized computer centers and system development staffs. With the advent of the minicomputer, decentralization of both functions has begun. This means that all departments in the telephone business will have to develop expertise in the computer area.

We will continue to build large data base systems as a central reservoir of information. However, the algorithms operating on the data will probably reside in small computers at the various operating departments.

Some of our super larger systems have caused employee and management problems in operation and maintenance areas. Employees have claimed they are slaves to an inanimate object. The machine schedules its own work, tells the operators when to mount and dismount data, and when running well tends to lull its keepers into a false sense of security. When the machine fails all hell breaks loose! Mean-time-to-repair is usually good—mean-time-to-restart is something else again. Restarting a multi-task system often requires an inordinate amount of time and money. In addition, managers in our operating departments are often disillusioned about centralized computing centers because they feel they are being held accountable for work over which they have no direct control. Therefore, where economy of scale was a prime motivator to install large multi-processing machines, it now appears that at least in some instances we have reached the point of diminishing returns.

However, it is clear that the use of small computers to assist in day-to-day work activities will expand greatly in the next decade. The availability of inexpensive data processors, economical input terminals and effective high-level languages will explode the use of computers in every segment of American life.

In addition to expanded use of high-level programming languages, you will see more and more micro-programmed machines—that is, machines wired to perform repetitive tasks (like an adding machine). Only these machines will retrieve data, selectively route information, perform measurements, etc., based on the user's input variables.

In the telephone industry the new electronic central offices are designed to allow the customer to transfer calls to another phone if they are away for the evening. This is a form of reprogramming under the control of the customer.

Looking at the business in the future, tomorrow's managers must be capable of managing in a computer environment. Today they are, too often, captives of the computer. Managers must learn to define what they want from the computer. Ill defined jobs are the biggest single cause of expensive cost over-runs in program development and on-going operation. The manager must know what he wants as an output from his computer systems. Not in hazy generalizations but in specific terms, because in computer technology there is no such thing as a vacuum; computers are yes/no machines. If the manager does not provide specific directions, the programmer will. The machine will not operate without direction.

The computer industry is not unlike the automotive industry of 50 years ago. It took several decades before the average citizen could afford a car. Today when an auto is generally available to everyone, there are still some people afraid to drive.

The same elements that made the automobile a mass consumer item are present in the computer industry today. Mass production resulting in lower prices, technological improvement resulting in greater reliability, and easier operation resulting in broader market participation will cause the change.

The secondary effects of the automobile had a profound effect on the American society—employment, mobility, the suburbs, etc. The computer revolution will undoubtedly have a similar effect.

As an example of what you the general public can expect in the future, earlier this month a Seattle firm introduced a unique service that allows users to pay some of their bills by phone. It is the first such service in the nation.

Telephone Computing Service, a subsidiary of a Seattle bank, offers its customers with touch-tone phones not only a way to pay bills with a few simple punches on buttons, but also services such as family budgeting, personal calendar reminders and an income tax data file.

With this service, called "in-touch," a customer's touch-tone phone even becomes a calculator which will add, subtract, multiply, and divide, with an immediate answer by computer voice.

Here's how it works:

The customer places a special guide panel over the touch-tone buttons which will enable him to reach a computer. After the customer punches in a private account number he or she uses number codes to signal which account is to be paid. For example, the user would push 12 for the gas company, then punch in the dollar amount.

After each transaction the computer voice repeats the order to insure against mistakes. If the figure is wrong, the customer pushes an erase button to cancel the transaction.

Every two weeks the customer receives a printed report of transactions. This same report also reminds users of all the other things the computer has been asked to bring up, such as birthdays, insurance premium due dates, anniversaries, etc. For a $6.50 service charge each month, the customer gets 100 minutes of computer time.

About 30 major businesses in Seattle, including Pacific Northwest Bell, other utilities and department stores, now allow bills to be paid by this method.

Each user has a personal code number which prevents accidental access to his account by another user. Privacy is guaranteed since all reports are tabulated and stuffed in envelopes by the computer.

Pacific Northwest Bell personnel worked with the bank subsidiary three years in developing the service.

On the work front, the computer will be used as casually as the telephone. Computation, retrieval, distribution and control of data will be done by the masses rather than a few highly specialized experts.

The Bell System expects a threefold increase in voice and data messages by the 1980s. To give you some idea of the magnitude of this projection, this year we will handle close to 150 billion messages. We are moving to meet the expected demand with the introduction of two new long distance transmission systems. One is a revolutionary millimeter wave guide system which can carry up to 230,000 messages simultaneously through a precisely

dimensioned underground tube. The second is a domestic communications satellite system to serve all 50 states, Puerto Rico and the Virgin Islands. If approved by the FCC, the satellites will be leased from the Communications Satellite Corp. and connected to earth stations which we will build. The satellite system capable of carrying 43,200 simultaneous messages will further increase the reliability and flexibility of the terrestrial network.

To sum up, let's review briefly what I've covered.

1. The computer technology will become broadly available. Most everyone will access a computer during his day-to-day activity.
2. The big growth in the computer market will be in the "mini" computer area. (Mini in terms of size and cost not in computation of logical capacity.)
3. The concept of "economy of scale" is falling into disrepute because of the high overhead cost and lack of broad management control over the large centralized computer complexes.
4. Large multi processing systems in the future will tend to be "data library's" or "data controllers," where the small computers can locate data residing in other small computers.
5. People will have to be trained to use the computer resource. In the 80s this training will probably begin in primary school. So beware! You know the trouble we've all had with the "new math" the kids bring home today.

Tomorrow your kinds will probably be asking you to assist in a programming problem.

With respect to the National Classification Management Society I believe that you will be able to have access and control of data where you need it by use of the minicomputer technology.

A Central reference library will probably be a large multi task machine that the minis can talk to when looking for data not in its own data bank. I believe the local minicomputer will use cathode ray tube devices for I/O terminals thereby eliminating the need for "hard copies." When printed copies are needed there will be photocopying devices available at a secured terminal. And, of course, the computers can be programmed to list documents that should be considered for reclassification or deletion from its files.

I believe NCMS is on the verge of a major break through in classification management. At times you may feel like the guy during the French revoluation who was running down the street tired and bleeding and was stopped by a concerned citizen and asked "what the trouble?" He replied, "see that mob two blocks ahead? I've got to catch up with them. I'm their leader!" ■

PROGRESS AND EFFECTS OF IMPLEMENTATION OF EXECUTIVE ORDER 11652 AND PROJECTIONS FOR THE FUTURE

Mr. Jack Robinson,
Center for Naval Analyses

Captain Richard E. Myers, USA,
Security Policy Officer, Office of the
Assistant Chief of Staff for Intelligence, USA

Mr. Daniel J. Dinan,
Deputy Director, Security of Military Information
Division, Office of the Chief of Naval Operations

Mr. Lawrence C. Myers,
Chief Classification and Information Security Branch,
Office of the Inspector General, USAF

Mr. Arthur F. Van Cook,
Acting Director of Information Security,
Office of the Assistant Secretary of Defense
(Comptroller)

Mr. Robinson: This morning we are going to an unstructured discussion approach on our topic. It is expected to be interacting with you as participants as well as the panel. We will be addressing questions for the panelists here as to what actions, what things and aspects have been covered, are being covered, are being reviewed or considered in the total program. As points arise, for example, and you have a question that has not been answered or which you would like to pose on any related topic, feel free to ask it at that time. The panelists are prepared and are interested in responding to particular questions that you may have. We have some prepared, just to start the ball rolling. And they may cause you to think of others.

To establish the frame of reference we might ask, where are we now in respect to Executive Order 11652? We have stated that an interesting aspect of our having this particular seminar now is that we are essentially at the first anniversary, of the Executive Order.

But is this really true? All of us, I think, recognize that the statement is perhaps not quite accurate—not quite accurate from an operating point of view. Yes, the Executive Order has been out for a year. Yes, interim procedures were published and arrived, let's say, either on time or shortly after time, and have, in essence, been arriving ever since. But for many of us the actual implementation has been a continuing process which is by no means complete.

The implementing directives from the several services of DoD to the Information Security Regulation were not really in hand until much after the Order's effective date. That's understandable too. It's not a point of criticism; it's a point of fact. It's a fact that we didn't have them. It's a fact that the Industrial Security Manual changes are not literally out yet. But they are intended. We have had advisories, we have had interim changes, we have had a lot of things. But it isn't correct to talk in terms of our having been operating for a full year. That's simply inaccurate. We haven't. We are still evolving.

So this is the frame of reference within which we will pose some of these questions. And the panel will help, I believe, in interacting both among them and with you to make this productive- let's ask the questions: where are we; how are we doing; and what are some of the effects as we see them now?

One of the things that Dr. Rhoads mentioned yesterday which we hope was a plus factor in the Order was the cutting back on the numbers of individuals having

original classification authority. He stated the percentages and so forth as to the reduction for DoD and CIA separately, some 60 to 70 percent, large reductions in the Top Secret classification authority, and so on.

The practical effect of this is a question, however, and I wonder if, for example, it has indeed reduced the volume of classified material.

How do you feel about it in the Air Force?

Mr. Myers: As far as the reduction of classified material, we haven't seen any substantial reduction in the amount of it. Certainly we have seen a lot of good decisions that are made. We have seen many people who would have classified rather casually before pulling themselves up short for lack of authority, and sometimes when they have checked with somebody with proper authority have found that they couldn't. We have had a major argument that we can use in dealing with staff and command, with anybody in the Air Force or elsewhere in the Government, as to whether something should be classifed or not; the very clear position of resolving conflicts in favor of not classifying has sunk in on people and it has had some effect. But I would guess that we haven't seen a 10 percent reduction in classified material if we were to try to guess in quantitative terms.

As far as the numbers of people who are classifying there has been a very substantial reduction. We have some figures here on that.

Mr. Robinson: The Army or the Navy, either one of you, how do you view the numbers game, if you want to call it that, for volume?

Mr. Dinan: Well, I guess the Navy has the same substantial cutbacks on the number of classification authorities as the other departments. We went from approximately 4,100 to 539, so that's a major cutback of about 85 percent. But of course all of you appreciate what we're talking about in original classification authority and we're not talking about derivative authority.

I guess I'd confirm what Larry Myers has to say about what happened in the Air Force. The decrease in original classification authorities in the Navy has had a psychological effect. People who may not appreciate the difference between derivative classification and original classification authority are doing a lot of thinking when they see they are no longer on the list for classification authority. Even though they still have authority to wield a stamp under the derivative concept, it has caused people to sit back and think about classification more and see if they have the right classification source and the right classification level.

Again, it's a difficult thing to measure to what extent there has been a decrease in the volume of classified information. We don't have any specific statistics for you.

Mr. Myers: Dan, I might pick up one point that you have there about people sitting back to think.

I'm not a great believer in the idea that numbers of people with classification authority has much effect, at least not at the level of Air Force and much less as you get down to the command, and very little when you get down to bases or when you get to industry, because the classification is derivative. I'm afraid if we get right down to it, the effect of the numbers of people who have authority is not going to be too significant unless the classifications that come from higher level are lowered.

But to some extent experience has shown that I have been wrong in thinking that this was just a numbers game with no significance. We have had people who have come in to us and said: We're in a bind here; we can't get our job done because we don't have classification authority out here; we're being forced to run things up to a higher echelon. So perhaps it has at least some practical importance.

Question: I have a question I'd like to direct both to Mr. Myers and Mr. Dinan on the figures for reduction in the volume of classified documents.

I wonder if that was just at the headquarters level or have you taken into consideration the Navy and the Air Force, all down the line, as to volume?

Mr. Myers: As far as our figures are concerned, first of all let me say they are top of the head guesses. I would say less than 10 percent and if someone wants to say that it is not more than 2 percent I have no way of rebutting it. What I am saying is it's not any major reduction. When I say that it's not a major reduction I am basing that on the things that we see from the field, the guidance that we have reviewed from the field, and what passes in the headquarters. It's a general statement but it's not based on a statistical measure.

The current guidelines didn't really have a lot of effect until the DoD regulation went out into the field in October. We don't have figures to show anything since then. In fact, our figures unfortunately are bulk—so many cubic feet—and although we could draw a comparison when they come in, I'm not sure what it would be worth.

Question: I was wondering if you attribute some of this small percentage to the inertia of the system, that people just haven't yet gotten with it?

Mr. Myers: You mean as to why it isn't a larger reduction?

Question: Yes.

Mr. Myers: As far as Air Force is concerned, I think it's because all of us have been so busy adopting the new system that we haven't made the most of it. Security effectiveness dropped due to program changes and confusion for several months.

We're now about at the same level as prior to the changes, but we have a number of actions that we can take to improve the situation which simply couldn't be taken until we got out of the initial period of mass confusion. But inertia or difficulty in adapting has been a part of it.

Mr. Dinan: I don't want the Air Force and the Navy to monopolize this so I'll just make a quick comment.

The statistics I was giving were not any statistics on cutbacks in volume of classified information. They were figures on the number of people that have original classification authority in the Navy. So we really have no feel as to whether there has been a cut back.

Mr. Van Cook: I'd like to make a comment, Dan, about the field level. A few elements did feed into the Pentagon in March. I'm talking about Top Secret now, reduction in Top Secret holdings. I talked with the person who was putting figures together and I think there was a substantial reduction in Top Secret. We're approaching 30 to 33 percent, varying with different departments. Whether or not that was a result of the Executive Order or just a general drive to cut down or not, I don't know.

Mr. Dinan: That was an inventory type situation. OSD went out and said take a look at your Top Secret

documents and see how much you can cut them back.

Mr. Robinson: That wouldn't necessarily mean that new things were being created at a slower rate, not necessarily at all.

Mr. Myers: I think it reflects a security awareness that may not have been evident throughout Government prior to 11652.

Question: Does anyone on the panel have original Top Secret classification authority?

Mr. Myers: Personally, do you mean?

Question: Yes.

Mr. Myers: I don't have any classification authority personally.

Mr. Dinan: Neither do I.

Member (Mr. Chelius): You know, I see a problem. I think you probably all know my views, and I don't want to get personal, but unless the people that are responsible for classification management are given the responsibility for having original Top Secret classification authority, then the decisions are being made by other than security people. Really we have very little influence—when I say we, you in Government have very little influence on those decisions. They are made by the technical people who I believe are prone to want to make things—put them in exemption category 3, make things classified longer, perhaps higher.

When you get the authority to say to the technical people, "All right, we're going to sit down and review this particular project or program," then I think you're going to have an effective program; when you actually get involved in the decision making as to whether materials will go in an exemption category or whether or not it will be classified Top Secret.

Mr. Myers: There are two parts to that. One is, of course, you know we're involved. The other part, on the authority: our feeling is that there is enough push in the direction of classifying so that we don't need any authority to add to it. What we need is a declassification authority.

Question: Well, you can't have one without the other.

Mr. Myers: We take the position that you can have, on the basis of the Executive Order and the DoD regulation, and in fact have assigned to our own office the authority to declassify information that we did not originate—information from any place in the Air Force.

Now that authority has a few strings tied to it but roughly it says that we can declassify information throughout the Air Force if we have taken into account the views but not gotten the concurrence of, say, the field elements, and coordinated in the staff; and further that if we're sure of our ground and willing to stand on it, that we can declassify without coordination with anybody.

So we feel the authority to declassify is what we need really, and that we do have.

Question (Mr. Chelius): Doesn't that relate primarily to older documents?

Mr. Myers: No, that includes current documents. And we have gotten one other thing. We have required that each of several of the air staff elements designate one or more individuals, generally a very small number, one, two, or three, who have the same authority that we have. Authority is not a binding problem on declassification in the sense that it used to be. You still have fear, which is a big barrier.

Member (Mr. Chelius): I think maybe we can get into specifics then. I am aware of several situations. I'll relate one of them, where a particular item of information came out in a guide as Confidential. And we wrote a letter suggesting that it should not be classified, much less be in an exemption category. That letter was taken over to a Lieutenant in a project office and he said, no, it has to be classified. The response to us was, well, we've talked to Lieutenant X-Y-Z who says, no, that must still be classified.

To me that indicates that it's not the Top Secret classification authority, the person with the authority, that's making the decision. It's still the project officer or the individual in the project office; which in some respects means that the classification people aren't exercising independent judgment but are relying solely on the technical people, who don't have the authority either.

So I think some effort ought to be made to pull some type of internal procedures together so that the people with the appropriate authority are making the decision, or vest in the classification office the right to make those decisions.

Mr. Robinson: A great deal has been made of the fact that now one must be able to identify who did the classification. This is a procedure which is prescribed by the Executive Order and the implementing directives, and we find now the "Classified by" line on all these little stamps that we're using.

What effect has this had in fact? What would you say with respect to Army, Dick?

Capt. Myers: Well, I think that the basic three questions, the two previous questions and this one, tie in very well together in that the reduction in the number of people with authority to classify, as I see it in the Army, has really had no effect on the volume of classified material produced. The effect has been to bring an awareness to this act of classifying. The initial classification decision is a very important part of the new order. That's where the emphasis lies.

As to where the authority should lie, we feel it should lie at the level of responsibility, the highest possible level of responsibility, so the individual responsible for that decision makes it based on staff input from all of his command, not just the security office.

Question: Dick, do you think you get a better decision at a high level than you do at a low level?

Capt. Myers: Well, if we can get the emphasis *and* the decision made at that level based on the information that he (the classification authority) should demand before he says yes or no, we will have a better decision, because it will be analyzed in detail before it gets to that level. Through this process he will have the information on which to make that decision.

The impact of the "Classified by" line of course is the same thing. The people are beginning to realize that by putting their name on that "Classified by" line, it's coming back to them. There's an offshoot of this on record requirement, where he has to justify his classification and identify himself. This is a required part of the record. I think this is where the impact is going to be measurable in the final analysis. We can't see the impact now in tangible numbers.

We're going to see the results of this in the next couple of years. The purpose being served right now is to focus attention on it. We didn't have attention on it before and it's taken a year to get that attention under the new Order. Although, still, in some cases we find we don't have it and we bring it in through staff action. But that's where the

impact is going to be. We're just now beginning to see some tangible results.

Mr. Robinson: I wonder, Art, if you've had any reaction, let's say, from OSD itself as to their views as to the utility, the effectiveness, and how that particular aspect is working.

Certainly we can imagine that, in the complex papers which are created at OSD level, one is establishing policy even in the paper; guidance, if you will. Have you had any feedback of note in this connection?

Mr. Van Cook: Yes, we have. First, I'd like to comment on the first part of this matter which was the reduction of Top Secret classification authorities. We have had a 70 percent reduction of classification authorities at all levels in the Department of Defense.

Now, under Executive Order 10501 we had something like 30,000 people that had classification authority. Right there on the spot they could make classification decisions. There are now less than 9,000 throughout the Department of Defense—out of 2½ million people only 9,000 can make original classification decisions. The theory is that if you reduce the numbers of original classification authorities, it should have the effect of reducing the volume of classified information created all over the world.

Now bear in mind this is very young. This went into effect in the Department of Defense on July 15, 1972 by the issuance of DoD Regulation 5200.1-R. By that time certain classification decisions had already been made and they were issued in the form of security classification guides and DD Forms 254, to contractors.

Consequently, I don't think any reduction in volume or numbers of pieces of paper is perceptible at this stage of the game. There's no way of knowing. Further than that we have no comparison. We do not have any figures available to us to know what was out there before, on what was being created on a daily basis. Therefore, no matter what we get now in the way of statistics there is no way to compare. So we have to gather statistics now and compare later.

At the moment, it's just a matter of crystal ball guessing whether we're reducing the numbers of classification decisions. It is going to take time to find out but we would hope reducing the number of classifiers will make classifications a little more difficult and effect reductions.

Larry pointed out situations where people are saying "It's difficult for me to classify; I have to go up to see the official two levels above me to get a classification decision." Well, fine. We think the higher level you go to get that classification decision, the better it is going to be massaged and we may wind up with no classification rather than a classification. So we would hope that the reduction of classification authorities would have that kind of effect.

With respect to the "Classified by" line, we find that this is another area where it's having the effect of an individual thinking before he designates an official by title or position to be responsible for the classification of that document and filling it in on this line.

We have already inspected some 16 major commands and we find that the filling out of this "Classified by" line has some effect in the Department of Defense. In industry I don't think the "Classified by" line has any impact at all, and shouldn't have. The purpose of it really is to establish an audit trail, so that if a classification is questioned, you would be able to get to the person that made the classification decision. And it does that kind of a job for industry—period.

Within the Department of Defense we find that when an individual classifies and has to fill in the "Classified by" line, he's considering whether he wants to put his boss's name on this particular document as having classification responsibility. I believe that we have seen in our travels that it has an effect on the classifier. He is at least reexamining the classification to determine whether it's accurate and timely.

Member: I'd like to make two comments if I may. I think the reduction of classified information, the only thing you're going to reduce—if you're involved in classified work, you're going to write just as many documents or reports whether there are 3,000 people classifying them or 30,000. The only reduction you're going to get are those that should have been unclassified and semi-classified to start with. That's the only reduction you're ever going to get—unless you cut out research.

Mr. Van Cook: Well, let's examine that particular comment. If that's what you think is going to happen, that's exactly what we want to see happen. You're saying that if a report is written and it's either overclassified or has unnecessary classification, it means that that classification is going to be removed. That's exactly what we're looking for.

Member: That's right. A very small part of the overall amount.

The second thing is there's too much mix up between original classification and derivative classification. I doubt if there are five people in this room who have every seen a document that's got original information in it and there are no classification guides anywhere as to how to classify that.

Mr. Van Cook: Well, I would differ with you there. There's very little guidance on operational matters such as created by the JCS, for example.

But, in the technical area and in industry, we do have—for projects, programs, systems—classification guides which identify items of information which are classified at particular levels. But in the area of operations and planning, there is not a whole lot of guidance, so that you do get quite a bit of original classification in this particular area.

Question: Isn't that a very narrow area?

Mr. Van Cook: I think not. I think it's a broad area. I also think that you have to add intelligence which is another area where there is not a whole lot of guidance when original classifications come into play.

Mr. Robinson: If I may pick up on that point. For example, if you're going to design a new weapons system and have to be in context, you make a proposal that relates to an operational capability. The operational capability has got to relate to a mission function of one of the services. Your statements as to the system's utility have got to involve operations.

And when I say there isn't much guidance in the operational fields, that is with an exclamation point. In the intelligence field there isn't any, absolutely none.

So these things creep also into the documents which

must be prepared under the system. Does anyone want to comment on that?

A representative from industry, Lockheed?

Member (Mr. Daigle): Yes. Many times we come up with new ideas and new concepts for application. We don't know whether the Government is going to accept them and if they accept them whether or not they're going to consider them sensitive enough for the various classification levels.

So our approach then, the only one we have under the ISM is to mark it interim classified and send it in, hoping that the agency that we give it to will make a classification statement on it and send us something back which tells us how to classify work we've been doing.

We got a comment from one agency contractor (not the armed forces) who said, "We won't accept that; we'll send it back to you; classify it what you think it ought to be and we'll correct it for you." Now, on what basis do you classify what you think it ought to be? As I say, it wasn't a military person, but it's an indication of some of the problem we're having in communications directly with industry in these operations that you're talking about.

Mr. Van Cook: I think the guidance on which to make original classification decisions are the principles and criteria laid out in our current regulation which were developed by George McClain and Don Garrett some years ago and incorporated into 5210.47 for the first time. These are the kind of things they rely on plus the definitions *per se* of Top Secret, Secret, and Confidential. But it's a matter of judgment, reasonable judgment by reasonable people.

Member: Those are not quotable authorities in the "Classified by" lines.

Mr. Van Cook: True. We're talking about original classification decision. I say that this is the kind of guidance that original classifiers are relying on in these fields—I'm talking about the foreign relations field, operations field, and the intelligence field.

Mr. Robinson: Somewhat in the same context, Dr. Rhoads pointed out and there has been much discussion on the effect that, under the new order and the new approach, we have changed our traditional view from, "When in doubt classify," to, "When in doubt, don't." Use the least restrictive. Keep the classification to the lowest level: reduce, change, declassify. This is the current emphasis and it has been restated many times.

Has this approach been accepted among the agencies? Is there any evidence to suggest that in fact it has?

I wonder, Dan, do you have any views concerning Navy in this?

Mr. Dinan: I think many times there is too much emphasis as far as I'm concerned on the original classification authority. Basically, according to the regulations there are two types of DoD classifiers, derivative and original. I think the really important aspect of the new program is the new concept of when in doubt take the least restrictive classification or don't classify it at all.

When you have somebody who has a classification guide in hand or who has a basic document in hand that's classified and he is originating a new piece of paper, he has to make a subjective judgment many times as to whether that should be classified. And, again, the new concept of the Executive Order is when in doubt we're supposed to pick the least restrictive safeguard, the least restrictive protection.

A thing that is extremely difficult to change is the mentality of people in the armed forces. We've got, I guess, about 900,000 people in the Navy, 530,000 in uniform and the rest civilians. That's a lot of people to change. People who have had a long tradition of overclassifying.

We find that this new concept of classifying at the least restrictive level is accepted by people when they are talking about somebody else's classified information. But if they're talking about their own classified information under their cognizance, they don't like this idea of when in doubt take the least restrictive classification. We find that in our own office and we find it all over the place. Perhaps we haven't highlighted this enough that there is a new concept.

Some of the words that the President used when he put out his press release in connection with the Executive Order are pertinent—he said that in the past people classified based on whether there was a remote chance it might hurt the national security, but now there has to be a reasonable expectation that it would hurt national security. I think that concept hasn't gotten across as far as the Navy is concerned, and it's a concept that we're going to hit harder on.

Mr. Robinson: In that connection, by the way, there has been a great deal of controversy and talk on the change in terminology from national defense to national security. As a practical matter, do you see any real effect that this would have, just looking at it from a nuts and bolts angle; has it really made any difference as far as the classifier is concerned?

What do you think of that?

Mr. Myers: I was about to say that I don't think national security is really a legitimate term. It appears, but it appears only in the sense that these things are "now and hereafter referred to as national security." From our standpoint we feel it's important that people get back to military operations and foreign relations, which are the terms that are covered by national security, because as we read every day in the newspaper, national security is getting interpreted very widely by many people for many purposes.

Mr. Robinson: Has it really changed the character? Do you feel the classifier now has a larger scope because of the terms here?

Mr. Myers: I don't think that the terms or the definitions either one have made any practical difference in Air Force at all.

Mr. Robinson: What about Army?

Capt. Myers: No, we use this as a collective term.

Mr. Robinson: Question? Comment?

Question: I've heard the term derivative authority. I thought the abuse of the old system was corrected with this new order. The derivative authority is where all the trouble occurred. If a person has the authority, he *only* has the authority. No one else has anything derivative from it.

I've heard each panel discuss derivative authority. Where do you derive authority? You may have an assigned responsibility.

Mr. Myers: I don't think I've said anything about derivative authority.

Mr. Dinan: I guess I purposely said it to stir up a little trouble.

Really, I think, derivative classification is still continuous. The regulation says that either you make an original decision or you make a decision based on other guidance or other sources. Obviously if a classification guide comes out and tells people what they want classified, at what levels, then there will be countless people that are going to be producing papers based on that guide who will be applying the derivative marking.

Would you have a suggestion as an alternative to that, if we did away with this sort of approach?

Question: Well, I think one of our difficulties in industry, and particularly with your branch of the service, you put some screwy code down and not even the Navy knows who it is, and we take it as gospel and classify it by OPPP-7. We don't know what that means. We don't even know who OPPP-7 is; you can't find him on a list.

The way I view the Executive Order, 8,000 people now have the authority to classify and no one else may classify. People may apply classification markings but I don't think that means they have any classification authority.

Member (Mr. Garrett): I think it's not the matter of authority but as you did mention it's a matter of responsibility.

Anyone who is dealing with classified information has guidance which says it should be classified at a particular level. He must make a subjective determination that the information falls within that guidance. It's his responsibility then to classify it according to the guidance that he has.

Another point I'd like to make before going further is on the question about the national security, national defense, foreign relations.

Please note the Department of Defense since 1964 has included foreign relations in with the term "national defense," but it was always stated foreign relations that affect the national defense of the United States.

Now 11652 recognizes specifically that foreign relations and national defense both are classifiable subjects—or reasons for classification, let's put it that way—and uses the term "national security" as a collective term.

Mr. Myers: I'd like to add that in other terms you can say that there is no such thing as a derivative authority. There's a responsibility to act on a decision that has already been made, but the problem is that no decision is ever that clear.

If somebody makes a decision, let's say, that in an office you will charge to petty cash those items which are trivial and daily and have to do with the administrative supplies, then somebody still has to sit there and decide, is coffee an administrative supply, is stationery, and how about messenger fees and so forth.

So as you bring out and Dan does, people are still making decisions. I think part of the gentleman's question is do we want to restrict the use of stamps themselves or are we willing to say that since the man who is acting as a result of somebody else's decision is still required to decide whether it applies here or not and that we'll restrict that authority.

Personally I don't believe that we can go that route, because in the ordinary course of business everybody who handles classified material is apt to have a situation where he has to relay that same information to somebody else. This is a simple situation; what he's doing is literally acting on somebody else's decision. However, in another situation that frequently occurs, a man is trying to decide does this decision apply here.

Question (Rosanne Dial (SSPO)): I'd like to know if any of the members of the panel have figures on percentages where exemption categories are used, like exemption category 3 where this decision can be made?

Mr. Robinson: How is the exemption category aspect working, members of the panel? I'm not sure we'll get to numbers but we'll get the numbers if you have them. But is there a large tendency to retain the exemption status as opposed to the General Declassification Schedule? Does anyone have any feel for the trend at all at this time, or is it too early? What is the reaction?

Mr. Van Cook: I don't think we have any figures that would give you an indication of the percentage being exempted under category (3).

We just completed a statistical sampling in the Department of Defense of the numbers of documents created whether on the basis of original classification authority or the application of guides, on a daily basis for a one-month period. This was during the month of May, at the Top Secret, Secret, Confidental level, and what percentage of these went to ADS, GDS, exemption, or exclusion.

The results of that survey, with 76 activities participating in the Department of Defense, indicate that 7.1 percent are going ADS; 42.9 percent are going GDS; 43.3 percent are in the exemption categories; and 6.6 excluded.

Now, there is a danger in these statistics and I'd like to describe that for you. This was done on the basis of a requirement being considered by the ICRC for reporting on a quarterly basis all documents created from now on, along these lines: Top Secret, Secret, Confidential; how many go ADS, GDS, and exemption.

In this particular survey we asked that the three military departments—Army, Navy, Air Force—select at least two activities which handle a substantial volume of classified material for the purpose of a sampling.

In the Army two such activities were selected and it was either the headquarters of a major command or the whole of a subordinate command. For example, the headquarters of Army Materiel Command or the entire command of the Army Electronics Command.

The Air Force and the Army selected two such commands for this survey.

The Navy elected to select 72 activities throughout the world involved in across-the-board kinds of activities—some very high commands, medium commands, lower commands, offices, laboratories, and so forth, which gave us a pretty good cross-section of what's going on.

One of the activities that was selected by the Navy—just one—created 180 or 190 Secret exempt documents on a daily basis. We found that that particular activity created those documents correctly and they were properly exempt under the rules, but that they were short-lived documents. Two-thirds were destroyed within 90 days. The remaining one-third were sent to another command for evaluation and some percentage of those were destroyed. Those that remained were Secret exempt. So if

we had included that activity in this sampling, it would have raised the numbers of documents exempted, to maybe 60-some odd percent.

Now this is not an average DoD activity, not by a long shot. The figures show that. We only have about 40-some odd percent exempt on the average. We have these kinds of activities in the Department of Defense, that are in special projects and which develop this kind of information. To get an accurate sampling and try to project that sampling to the remainder of the Department is very difficult. It's very difficult indeed. We find that the gathering of these statistics is very costly, by the way.

Mr. Myers: What did you find in OSD itself, Art?

Mr. Van Cook: OSD was not one of the activities.

Mr. Dinan: I might comment, Art, since you've emphasized Navy participation in the sampling that the activities selected by the Navy were heavy producers of classified information, and they were also activities that you'd expect would tend to exempt the material more—intelligence activities, the Naval Intelligence Command, Naval Security Group, these sorts of activities.

To follow up on Van's point, you really can't make a judgment based on the figures that he gave out—what did you get, 43 percent exemption?

Mr. Van Cook: Yes.

Mr. Dinan: If you just look at the Navy figure, there's a 45 percent exemption. Some people might say that a 45 percent exemption figure is pretty low for intelligence and security group activities.

I would say based on those figures, as far as the Navy is concerned, there's too much exempting going on.

We have looked at a substantial amount of message traffic coming in to the Chief of Naval Operations and took a fairly good sampling of close to 1,000 messages. We found that the exemption ratio was about 26 percent.

Mr. Van Cook: I'd just like to make one additional comment on the figures that we're talking about in this statistical data sampling. We have not done this before. These kinds of numbers were not available to us. We again have no basis for comparison. We don't know really what the order is doing for us at this time. We would have to take the same sampling again and do it at another time, maybe six months or a year from now. The current sampling will establish a baseline for us. With future samplings, we will be able to get a feel as to whether more information is going into ADS and GDS by comparison.

Although we have the statistical sampling right now and we tell you that these are the results, we would hope that maybe in another year or so when we go back to these same units we'd find a whole new ball game, that there would be a very small percentage exempted and a very large number going into ADS and GDS. This is our goal anyway, and this is what the Order is designed to do and we intend to make it work.

Question (Mr. Rankin): Van, the 43 percent, I'm curious as to whether or not you're satisfied with the 43 percent. From your comments, I presume that you would like to see it reduced. Has OSD established any particular percentages?

Mr. Van Cook: No Dan—certainly I'd like to see it reduced. I'd like to see the objective of the Order reached. The overall objective of the Order is to maximize the amount of information given to the public. It is to me the same objective as the Freedom of Information Act. Certainly it's the ideal thing to reduce classification measurably. Let's knock it down, try to get more into the ADS, more into the GDS, if it's at all possible.

I certainly can't sit here in judgment and say that this is not realistic under the provisions of the order, or that the 43 percent rightfully belongs exempted by the terms of the order, encompassing all four categories. What percentage of this 43 percent is information that is protected by statute such as the Atomic Energy Act; what percentage of it is foreign originated; what percentage of it is intelligence sources and methods, I don't know.

I'm just saying that it would be our objective to try to reduce the amount exempted to meet the overall objective of the Order. Whether we can or not, I don't know. Maybe when we survey these same activities in a year from now we'll get the same answers.

Question (Mr. Rankin): Has any consideration been given to the life cycle of R&D? If the great bulk of material falls into R&D, technical information, it would certainly seem to me a great part of that is going to have to be beyond—say it's classified Secret—it would have to be beyond an 8-year period. But just on the surface I would think that a lot of material, 40 or 50 percent, might fall into that.

Mr. Van Cook: It's very difficult to put an estimate on that, but I would think that if the stuff that we're talking about here, this 43 percent exemption, is in the R&D area, it's probably in category 3.

Now we have gone out, as I have indicated and conducted a program review in 16 major commands throughout the Continental United States and Hawaii. We found out, for example, one major command has established what they call a challenge program. They're challenging classification—lateral, subordinate, and even those coming down from higher headquarters. In 56 challenges, 46 cases resulted in downgrading or declassification marking instruction or in a less restrictive classification or no classification at all.

Mr. Myers: We're happy with that challenge program but there is a better challenge program than our own, I think, going on in Navy. They have a pretty large scale challenge on messages, do you not, Dan?

Mr. Dinan: Yes.

Mr. Myers: I sincerely believe it's a better system than anybody else has set up so far, at least in the width of it. But I never happened to talk to anybody to question what their results are.

Mr. Dinan: What we're doing in our office is reviewing a selected sampling of classified messages that come in to the Chief of Naval Operations, and see what we think from a review standpoint as to whether they are properly classified or not.

One of the real pleasant revelations from that exercise has been the adoption of the ADS concept in the Navy as far as messages are concerned. We're running about 25 percent of the messages classified on an ADS basis.

This is an ongoing program where we actually review the message and come up with a letter going back to the command if we feel the command has made an improper judgment in classification.

Of course we don't have all the facts in front of us in

a situation like that. But in this letter to the commands we point out where we think they've done wrong, and we invite them to reclama or to call us. Our telephone number is on the form letter that goes out.

We've found that we're running across about 12 percent of the messages which appear to be incorrectly classified. If you take that sort of statistic and then take the statistic on the high rate of exemptions that are going on in the Navy and the Department of Defense, we have to assume there are a lot of errors being made. To assume that everybody has the word and is doing it properly is sort of an unrealistic attitude. We have a new program and still have a long way to go in our education process.

When I see figures in the Navy of 43 percent exemption in looking at the 72 commands, I say that's too much. And it's going to be cut back. It's obviously going to be cut back. Because obviously everybody doesn't have the correct word yet.

But the encouraging aspect we've had on these reviews is the ADS thing. I think we should look at this from a positive standpoint. That overall Department of Defense study showed that 7.7 percent or something like that of the documents were ADS. In the Navy we're running about 8 percent.

With respect to security education, we've opened up channels of communication between our office and the field by a hot line concept of making our telephones available and letting them know where we can be contacted. For a period of three or four weeks we got as many as 1,000 telephone calls. Over the year we've been getting several thousand calls. We write it in our regulation. We write it in our form letters. We write it in everything. If you've got a question, call us on it and we exchange ideas and resolve problems. I think that's one of the best forms of security education.

Another way of getting the job done is through monitorship and inspection. Besides monitoring classified messages, we're checking every classified instruction that's put out by the Chief of Naval Operations. If the instruction is classified, it is reviewed by our office to make sure it's properly classified before it leaves. So we're preventing a lot of initial over classification.

Member (Mr. Buckland): I wasn't going to ask a question. I want to make a couple of comments that I can stand on later today.

I heard the last comments, and I speak for industry and myself. I think that one thing that should be remembered, it's a long way from you members of the panel down to where we are, and there are an awful lot of people in between. But in this business of communication breakdown, I thought you might be interested in a small study. Recently we examined a number of current contracts in industry. I did one and then I added several other industries.

Out of 121 contracts that are currently underway in several major industries, 59 of them still cause us to put all of our information in those contracts in the excluded category. Fifty-three of those contracts allow us to use the exempt category. Only four out of the 53 give us a declassification date. Only 40 contracts out of the 121 have some GDS in them. None of them have any ADS. And when I say from GDS, if it applies to the whole contract, it's a small contract which probably wouldn't generate more than a hill of beans. If it is a large major contract then you'll find that maybe two items are GDS, and 50 items are X-GDS.

These figures now—this is coming down to us and I'm not talking about the number of documents that we are generating, as you are talking documents. I'm talking of programs and where we have to put the material.

The general consensus of industry for those whom I have talked to is, "forget GDS, it doesn't amount to a tinker's dam." Most of what we're getting in is X-GDS. And as I said, I have yet to see my first contract that has anything in ADS. Despite the volume of documents that we have, I haven't seen any ADS documents yet.

Mr. Myers: Dan Rankin raised the point of the life cycle on the period of time. Suppose the six and eight years were ten and twelve years, do you think you would find a lot more GDS then?

Member (Mr. Buckland): Quite frankly, I think you could get a tremendous amount of information that's available today and placed in X-GDS, could logically be in GDS. I think that the people are leery of the shorter span.

Mr. Myers: Also I think there's a psychological problem of biting off on six years.

Member (Mr. Buckland): I think it's psychological. I think they're not used to it.

Yes, in some research and development programs, major missile programs and things like this, I can see where six and eight years is not long enough. When you're doing the first advanced R&D program on a system and you're scheduling your production contract for mid-80s right now, six and eight years is not long enough. But that should only be applied in certain exceptional cases, and in those cases they could use the X-GDS very very logically if they will assign a declassification date.

But when you consider that only four contracts out of 53 that we studied give a declassification date for the X-GDS material, it means that they are afraid to do it, so basically the vast majority of the material is going right smack into limbo for 30 years either because it's still being excluded or because it's X-GDS without a date.

I just point this out because in industry the general comments that I've heard are diametrically opposed in a way to what you are saying. Although I agree with what you are saying, I think most of us here will agree with you, I want to stress again it's a long way from that table way down to us in the user agencies and there's an awful lot of interpretation and there are an awful lot of, I'll say, scared people that are putting out these instructions.

Member (Mr. Robert Neal): I'd like to further what he says in this application of exclusion.

Out of 240 or so classified contracts we have, I'd say it's about the same percentage. Many many documents and we're generating, hundreds of them, we're instructed to mark them excluded.

I think this is diametrically opposed to the whole philosophy of the Executive Order. Somebody just hasn't made a decision or has no intentions of making one. And it's just a blanket application through some of the user agencies to mark everything excluded.

Mr. Robinson: It looks like there's a lot of interest here, but one opposing point at the moment.

Member: I think that one point that's been overlooked

in all the discussion here is the mandatory annual review of DD 254s which go out to the contractor.

Logically, whatever term you want to use, much R&D data of necessity has to be put in the X-GDS because of your time frame. But as you go down the years there's going to be a point in time at which you can put a definite declassification date or put it into the GDS category. So if people would abide by the existing regulations and review each DD 254 for every contract at least annually and make a determination, I think that problem might go out of the picture. You won't have it.

Mr. Robinson: It would be easier to resolve.

Member: We've been watching this kind of come and go and we have a feeling, whether it's right or wrong, that after we get to declassifying the old group 4 documents we're going to show a large reduction in volume of classified documents. But, as our new exempted documents are produced, we're going to end up with more classified documents in our facility than we had before.

Member (Mr. Albert Becker): I'm from Georgia Tech and I kind of sit in a place where we do R&D before Jim and his crew get in on the ball game.

I'd like to say that generally I agree with what I've heard from the floor here. What I see happening to me is this: even where we have a program where we get GDS directives, because of derivative classification the new document becomes "excluded" and I end up with materials that are frozen; even when it's GDS on the 254s, I still end up with material in the excluded category.

I have only one contract where the work is original and the GDS intent is in fact functional. Somebody needs to look at this whole group 3 category of material.

Mr. Van Cook: We just approved a policy that's being disseminated this week, and I was going to touch on this at the conclusion of this session. We have dealt with group 3, and we have reinstituted the group 3 instructions as stated in 10501. What we're saying is group 3 information so marked will run its course. In other words, it will be downgraded at 12-year intervals as group 3 was previously. We're also saying that when you withdraw from your file or storage area a document which is marked group 3 there will be no requirement to remark it "Excluded" as we have before because the instruction on group 3 is clear: downgraded at 12-year intervals; not automatically declassified. That policy has just been approved and it is being disseminated this week. This then invalidates the current requirement in one of the 72-L letters that says you have to go back and remark all these.

We are also saying in our policy that, if you have already remarked it, the old marking prevails. You don't have to go back and do something else with it. If you've done it, it's done, and that's the end of it.

Member: The reason I make such a point of this, many of us have computerized systems. When we had the old group 3 every 12 years the computer would kick out a reminder to tell us it's ready for downgrading. With the advent of the new directive, many of us have already redone our computerized document control system, have taken the group 3 out and made it all excluded. Now we're going to have to go back and put the thing in again.

Mr. Van Cook: Well, you know, somewhere along the line you've got to take action. We have just been advised of a determination by the Justice Department that the Secretary of Defense could in fact do what we are doing now. The order came out, you know and said that this material would be excluded. We went that route. That's the way we implemented it.

But now because there's been a lot of discussion about it from industry and from people about this having the effect of freezing something at a particular level, which we didn't want to see happen, we raised the point and we have got a decision. The policy has been changed. It will be out very soon.

On the exclusion business, I'd like to add a comment. Many people are calling about a problem involving the issuance of guidance which says if you create something today mark it excluded because under the previous guidance it was group 3. Now that's wrong.

When a guide is created or when a guide is revised or a new guide is issued after June 1, 1972, the term excluded should disappear from the scene. Anything that was group 3 before or group 1 or group 2, whatever the case may be, the party that revises that guide or creates a new guide must bring the guide in line with the new Executive Order with respect to ADS, GDS, or exemption. Exclusion should disappear from the scene. I mean the word should be dropped out of the vocabulary as time goes on. It was only thrown in there to take care of an immediate situation. It was a temporary expedient but as guidance is developed now, anytime after June 1, 1972, no one should be saying anything that you create today should be marked excluded.

Member: I'd like to point out if you're going to reactivate the old group 3, that the directive establishing it has been canceled and so if you're going to leave it where it still says downgrade in accordance with DoD directive 5200.1, which has been canceled, that you need to have some different language to take care of it.

Mr. Van Cook: Well, that's not necessary—we have a marking on a document which is a clear instruction—you're just talking of mechanics. You're talking about a document that's already marked, with that old marking on it.

We see no reason in the world for a new marking because it happened to reference a canceled directive. The instruction is clear; and our rule, if you treat that document as a document which will be downgraded at 12-year intervals and not automatically declassified as the instruction reads on the stamp, you'll be in accord with the rest of the world. We don't want to see a remarking every time a group 3 document is taken from a file.

Member: I cannot resist making the comment that NCMS made a formal representation to DoD some time ago on exactly this process. I gather now that you are agreeing with us.

Mr. Van Cook: Yes.

Question: If I use a group 3 document as a source document, how do I mark the new document. Do I mark it group 3?

Mr. Van Cook: The beginning date for downgrading this document will be the date of the source material. I think the provision reads that you'll use the type of marking we now have for ADS, which would be downgrade to secret on a particular date; with the beginning date being the date of the source material.

Question: You're talking about creating a new document today from a group 3 source?

Mr. Van Cook: You would use the stamp we now use for ADS which says "Downgrade to Secret on, Downgrade to Confidential on, Declassify on." And you would insert the date for downgrading, but not automatically declassifying.

Question: The ADS stamp will always be less than the GDS stamp?

Mr. Van Cook: Well, I'm saying the use of a stamp that's in existence rather than having to go and purchase new stamps. There's no other way to treat that stuff if you want to mark it properly and let the recipient know what to do with the document.

Mr. Myers: In other words, if you have a group 3 document that's classified TS and the document is dated 1965, if would still be TS but you would mark in a format that would show downgraded to Secret 1977, to Confidential 1989, and then not automatically declassified. You'd just apply those dates to it.

Question: First, how many members of the panel are directly involved in the preparation of 254s?

Second, do you realize how many 254s now are going to have to be revised to put in what you just said? Because they state something else. So we're going to have to revise every 254.

Mr. Van Cook: There is a requirement for an annual review of the DD Form 254 and we may have to get another program going as we did once before for a mandatory review of these things on a special project basis. We did that over a 6-month period of time, every DD 254 was reviewed in the department and we asked for a report on the results of that review. From what I gather from the industry people speaking here today, these DD Form 254s apparently require a pretty good shakeup and we're aware of it because we've been around and we've been to commands and we've been to industry and we know that they are not being accurately prepared.

So this might be a good way to shake it out, and I'm happy to see it come down to it.

Question: I have in my notes a reflection that it's felt that going to the higher level for original classification authority will result in a better message--I believe Mr. Van Cook made some comment to that effect--thereby we will gain a better classification on a piece of material.

However, subsequently, I heard Navy and Air Force say that they found it necessary to implement challenge programs, and that of 56 messages or something reviewed, 46 were sent back with improper classifications. Now isn't that a little bit of a diametrically opposed philosophy problem there?

Mr. Myers: To pick up the Air Force part of it, I think what it shows is that people in the particular area of the challenges weren't making the best decisions originally.

Now we get copies of those challenges at our office. When you see a number of challenges in a given area, you put out some new guidance; which is what we did. In the same subject matter that was being challenged, I think I have seen roughly three challenges in the period of the last three months.

To the question whether you're getting better decisions or not because they go to higher level, I don't know whether you do or not. As far as I'm concerned it's an open question. It's an impediment which may have a positive effect but I really don't know.

The challenges certainly do indicate that some things are being classified that don't need to be. When you see the challenges--if you require copies of them to come in--you can take action to correct the problem, and in this particular case it largely has been corrected.

Question (Mr. Chelius): I'd like to go back for a minute to the "Classified by" line as it's used in industry.

I have noticed on several occasions that we have been advised, number one, the ISM says you use the 254 and the date, etc. We're all aware of that. But I notice in several instances where we in classifying material Restricted Data have been told to cite Army, Navy, Air Force guides or 254s.

We all know that Restricted Data cannot be classified by the Department of Defense as an AEC function and therefore I wonder why we are not citing the proper classification authority, the original source, which would be a joint guide, such as CG-W-3 or CG-WT-2, etc.

As an example, we had a 254 come in recently and it talked about rain, dust, and snow in relation to nuclear matters and it said classify the material as Secret Restricted Data. When that happened I knew that the people had not considered the proper policy guides to find out what the classification should be. Therefore, particularly with Restricted Data, I think if we in industry at least were told in the DD 254 what policy guide applies, then we would be more likely to challenge and get proper classifications.

Mr. Van Cook: Usually, in a DD Form 254 I think identifying the AEC guide would be all right if it's applicable to performance on that contract and it is made available to the contractor. Does that show up at all?

Member (Mr. Chelius): No. They just tell you to make it Restricted Data. They don't tell you what guide they based the RD classification on.

Mr. Dinan: Well, isn't it fair to say this "Classified by" line of the declassification stamp started out as an excellent idea but then it sort of got garbled as we developed the concept. For example if I create a piece of paper with Restricted Data on it and I'm classifying the piece of paper that I have created and I've got multiple classification sources, regulations say that I'm supposed to show the signer of that piece of correspondence. If that goes to industry, industry gets that piece of paper and looks for "Classified by," but doesn't see any basic sources. What he sees is the name of the individual who originated the intervening documents.

There is an audit trail, but the "Classified by" doesn't always show you who the original classifier was.

Isn't that a fair statement--correct me if I'm wrong--you can't look at the "Classified by" line and determine who the original classifier was.

Member (Mr. Chelius): That's the purpose of it though in the Executive Order.

Mr. Van Cook: The requirement for industry, as far as the "Classified by" line is concerned, is to identify the DD Form 254 as to the date and the contract number, those two things, and then if one additional guide is used, also to cite that guide. In the case you are describing here, it seems to me that you have a DD 254 which

identifies a particular item of information as RD. If you include that item of information in a document, the "Classified by" line which appears on that document which you create cites, in accordance with the rules, the DD Form 254 date and contract number. Now I don't get the point about an additional notation—why do you have to know about an additional guide for that particular kind of DD Form 254? What is the point you're making?

Member (Mr. Chelius): I'd like to know that the fellow that filled out that 254 at least consulted the major classification guide for the area.

Mr. Van Cook: Well, that is his responsibility and I guess you would have to assume that he had. Are you contesting the fact that the Secret Restricted Data is contrary to the guide itself?

Member (Mr. Chelius): That's right. That's absolutely correct.

Mr. Van Cook: Well, in that case why not bring it to the attention of your cognizant security office and ask them to look into the matter. You have a specialist out there who handles that, haven't you? If you happen to know that the classification in contrary to a guide, you shouldn't just blindly classify it on the basis of the guide without bringing the matter to somebody's attention.

Member (Mr. Chelius): We would do that. But I think it goes back to the basic thing of having DoD authority for Restricted Data. I think it should be an AEC authority based upon a joint guide.

Mr. Van Cook: Well, for the purpose I'm talking about, the "Classified by" line, the only requirement is to establish the audit trail. This we have done.

Capt. Myers: Is it ever authorized to put down a DD 254 date and contract number on the Classified by line for Restricted Data?

Member (Mr. Niles, DNA): I guess I'm as good as anybody to answer that question. In DNA, the contractor shows the DD Form 254, dated so and so, contract number such and such. The 254 lists CG-W-3, CG-WX-2, etc. More probably, he lists extracts from that, because we do not ordinarily give the whole guide to them.

Now I would hope that George would exempt DNA from this when he says "they." But I think what George is talking about here are some 254s which he gets with three or four items which say these are SRD without going back to say why.

But I think as far as we go, we list every one of those joint guides or guides which we have produced which are "derivative" from the general classification guide. This should be done, I believe, by every person who is involved directly in the formulation of DD Form 254s.

Question: I want to ask a question regarding the challenge program. Has there been any thought of challenging the classification guide, review thereof and challenge?

Mr. Myers: I don't know that you're speaking in terms of quite the same thing. In a challenge program, such as we're referring to, everyone is encouraged to challenge any overclassification he sees, willy-nilly, without needing to cite any guide at all.

As far as the guides are concerned, I would say that the state of review on those leaves a lot to be desired. The guides are reviewed, but frankly, they are not reviewed with as much detailed consideration as we would like. But every guide that is prepared in Air Force comes in to our office and how well we do with it depends on how much time we have to go through it.

Your point, I guess, is if the guides themselves are properly lowered in their classification requirement that you'd get a sizable result from that. And I agree wholeheartedly.

But that's something that has to be done in more than one office. It has to be done in the program office itself or done in one of the offices at Headquarters Air Force or at the major command level. Yes, we review them but, no, we don't think the review is anything comparable to what it should be.

We sat down the other day to set up some goals for ourselves in the next year, as we do occasionally, and one of our top priority goals is to give a better review to the guides. Because that way, if you can cause one piece of guidance to go down you may cause a thousand documents to go down. This should be a top priority in Air Force certainly and I would think elsewhere.

Question: Are you able to review them before they are published?

Mr. Myers: Generally speaking, no. We could require that, but without even getting to 254s we carry between 200 and 300 active classification guides that are changed perhaps on the average of two or three times a year. Now with some of those, there's a requirement that they come in to headquarters for review before publication. With most of them there is not and it's a post-publication review—management by exception, which reflects two things I think. One is the manpower needs and the other one is the desire to avoid holding things up by taking the authority away from the program office.

Mr. Robinson: Guides is an important topic, and I wonder if you might offer some observations, Dan, and Dick too, on the status of guides as you view them under the program; as to their quality, their improvement, their timeliness, or other points of that nature.

Mr. Dinan: Well, this is a high priority item with us. We just recently got the attention of the Naval Inspector General and the Vice Chief of Naval Operations on the classification guide problem. We hope in a week or a few days to have an approval by the Secretary of the Navy on a directive to Navy people requiring that this classification guide program go forward full steam.

What we found in our recent review of classification guides in the Navy is that we have approximately 155 classification guides and 30 percent of those are less than a year old. In other words, 70 percent of the existing classification guides are more than a year old and we find that unsatisfactory. In addition, the Navy's classification guide effort is unsatisfactory because there are many programs in many areas that don't have classification guides. We took a look at our 47 major weapon systems programs in the Navy and found out that about 55 percent of them had classification guides; the others didn't have classification guides.

So the directive that we hope to be signed out at a high level in the Navy is that all program sponsors and people involved in areas that require classification guides will be required to identify them to our office and we will have a rather strict monitorship on a continuing basis. The clout that we always needed we hope will be written into this directive and we will have a mechanism for

putting activities on report to the Vice Chief of Naval Operations if they fail to do so.

That's the kind of clout that we need in these kinds of programs. I think you all have to realize that we're competing with an awful lot of other programs in the Navy. We've got programs on alcoholism, equal opportunity programs, safety programs, recruiting programs—all sorts of programs that everybody thinks are of very high priority. It's difficult for us in the security area, in the classification management area, to compete with these things. What we have to do is get high level interest and get effective monitorship. We've got to get a program by which we can put people on report, and then they'll be concerned about keeping their classification guides up to date.

It's a difficult job and a manpower problem but we hope we can do it.

Mr. Robinson: How about Army?

Capt. Myers: Well, I think as far as the adequacy of the Army classification guides, you people are in a better position to judge whether they are adequate or not than I am.

What we're trying to do is to bring some more management control into the classification guidance area. We have asked our IG's when they go out to ask the people in Army field commands two questions. One question is: what types of information are there created within this command that you (the local command) need to issue classification guidance on; and when are you going to issue it? The other question is: what types of information are created in this command as a result of direction and tasking from outside that you were not given classification guidance with the tasking, and why haven't you asked for the guides?

On top of that we have charged the heads of the Headquarters DA staff agencies, functional specialists so to speak, with the responsibility for coordinaton and final approval of all classification guides. This is one of the major programs within the Army.

By putting that final approval authority at that level, we hope to be able to get all of the detailed analyses and the staffing requirements and all the threads identified: does this information need to be classified at this level; when can it be downgraded and declassified? We think that this type of analysis, the fact that the Head of the staff agency is responsible for the approval of that guide, and because the bulk of our Top Secret classifiers are at this level (there are only 58 of them in the Army) if it's got exempt information in it it's got to be approved by a Top Secret classifying authority—all this will give the Army the most accurate and adequate classification program.

So by having it approved at that level we are hoping that the question is answered somewhere along the line. We don't have information on how effective this is right now. We're still working at the action officer level trying to make sure that the staffing is up to that level. The approval responsibility lies there which means he's got to see it, he's got to approve it. We're hoping that this will turn the tide in classifications in the Army, the high level command emphasis on the subject of initial classification.

Mr. Robinson: One of the things we certainly want to hear a little bit about is the current thought and projections as they may be viewed at this time from OSD's point of vantage.

Mr. Van Cook: We have covered a lot of ground since Executive Order 11652 came out in June of 1972. The first order of business was to get the order implemented and get the rules out to people who could use them. That was accomplished with a single DoD issuance which was supplemented by the military departments.

Now, you people have been in the business long enough to know as I do that knowing the rules just doesn't make the ball game. It takes a good manager to run the team, in this case defense industry, to show good results. Once the rules are out and people have had a chance to work with them, then the emphasis has got to be on education and training.

One of the things coming down the pike is the establishment of an Information Security Management Course at the Defense Industrial Security Institute at Richmond, Virginia. This course has been approved by the Defense Management Education Training Board. It will be two weeks duration and will accommodate both industry and defense. It is intended to provide 20 resident classes a year.

We have been putting out and will continue to put out articles on the Information Security Program. They have been in such things as Commanders Digest, Defense Management Journal, just plain talk articles giving people the views of the top level people in the Department of Defense on this particular program, and showing the emphasis that these people are placing on this program.

In the way of monitorship, we have established in our office a division which is solely responsible for going out and conducting program reviews throughout the world, in company with representatives of the military departments concerned.

As an example, when we go to a command of the Army we invite a representative of the top echelon of the Army to accompany us. We get in there and see what's going on and report on it. Thus far we have gone into sixteen major commands throughout the Continental United States and in Hawaii. We have been to contractor facilities and we've visited with the headquarters offices in the military departments and defense agencies. We're getting a pretty good picture on what's happening and we're going to continue this program with more emphasis in the months to come.

So it's a matter now of education and monitorship. The apparatus has been established for monitorship to be effective all the way up the line throughout the military departments. There is a great deal of command emphasis on the program. The top level officials of the department are behind the program and are anxious to achieve its objectives.

The overall objective, as I mentioned earlier, is to maximize the amount of information that goes to the public, and the way to do that is to declassify more, classify less, and better safeguard that which remains.

We conducted a Top Secret inventory reduction in the Department of Defense and reduced our Top Secret inventory by 25 percent. This was the goal that was set for this particular 60-day project and it was achieved. We now have an inventory of something on the order of half a million documents throughout the Department of Defense in the Top Secret category. Something like

166,000 were destroyed and we think that this has the effect of reducing the risk of compromise of the information contained in this non-record material.

The Department of Defense Information Security Advisory Board is planning to be active in the months ahead in establishing programs for total declassification of projects, programs, and systems. We are going to try to identify entire programs, entire projects, and entire systems and review those with a view to mass declassification. This is an item that we want to get on an early agenda of the Defense Information Security Advisory Board in the weeks to come.

There has been a lot done but there is still a long way to go. We can see from the discussion here that one of our priorities must be the revision of security classification guidance now in being, and bringing it into line with the letter and intent of Executive Order 11652. We hope to accomplish that and have several meetings now established to get this job done. We'll be looking into that as a top priority item. ■

NEW INDUSTRIAL SECURITY POLICIES

Colonel Donald T. Clark, USA,
Chief, Office of Industrial Security,
Contract Administration Service, DSA

In February of this year, I had the privilege of addressing a Classification Management Workshop in Orlando, Florida. Members of your Board of Directors were present at this earlier meeting which was hosted by Martin-Marietta Aerospace. Right now I feel like I'm among old friends. While some of my comments from the February meeting will be repeated, a number of new considerations have appeared which I will address today for the first time.

With the emphasis being placed on the subject of classification management by Executive Order 11652, the Department of Defense regulation and the changes issued to the Industrial Security Manual, this seminar provides a valuable service to Government and industry.

The educational value of this seminar is an important adjunct to our everyday operations. Written requirements are essential in the classification management business but these words on paper will not get the job done by themselves. It takes people who understand the who, what, when, where, why and how of these requirements and then translate them into action.

The subject on which I have been asked to speak is New Industrial Security Policies. A learned philosopher has said, "There is nothing new under the sun." I wonder if what we sometimes call "new" isn't really a renewal or change of something already in being. For example, the Defense Industrial Security Institute is a new identity but, with a mission similar to that formerly assigned to the Industrial Security Committee of the U.S. Army Intelligence School. As a field extension of the Office of Industrial Security, the instructors of the Institute are now dedicated solely to the Defense Industrial Security Program.

The charter we have given to this Institute is designed to make it become the "academic center" of the Defense Industrial Security Program. We look to the Institute, its faculty and its students to develop new ideas to reach over the frontier, to write learned articles and to do all the things for our program that a great university does for our society.

As some of you are aware, there are plans underway to expand the mission of the Institute. Of most interest to this society is the development of an Information Security Management Course. For the first time, the Department of Defense will have a formal training course for those engaged in the classification management function as well as for the security manager with overall responsibility. We are enthusiastic about this effort. From the reports I have received, it would appear that this new course is moving rapidly from the drawing board stage to the point of realization. Approval for the development of this course was granted by the Defense Management Education and Training Board in May. During the week 11-15 June, a joint service task force met at Cameron Station to draft the broad program of instruction.

INFORMATION SECURITY MANAGEMENT COURSE
(Two Weeks)

TRAINING IN: Classification Management Safeguarding Classified Information

FOR: DoD Military and Civilian Personnel Responsible for Administering Program

Industry Personnel Responsible for Application of Classification (one week)

While the course is designed for Department of Defense Security managers, it is expected that industry representatives will be offered that part relative to classification management training. This could be accomplished by expansion of the present one week Industrial Security Management Course. We would propose to make classification management a separate presentation to enable the alumnae, who have already taken the Industrial Security Management Course to return for this specialized training.

WHAT THIS MEANS TO INDUSTRY

1. Academic Base for Classification Management Training
   - Augment present ISMC
2. Long-Range Benefits
   - Better classification guidance
   - Uniform appreciation of security procedures

The potential long-range benefits of this new course are many . . . uniformity; better classification guidance; an academic base for this safeguarding of classified information common to Government and industry. These are but a few of the major benefits to be realized.

Some of you may also be aware that we are tasked with another new mission . . . the conduct of physical security surveys of key facilities . . . presently known as the Industrial Defense Program. We expect to complete

the functional transfers by 1 October 1973. With this program comes an educational responsibility. Since our educational base is the Defense Industrial Security Institute, we would naturally place the new physical security training requirements there.

INDUSTRIAL DEFENSE PROGRAM

Physical Security Surveys of Industrial Key Facilities

- To assure uninterrupted production capabilities of industrial facilities and their attendant resources.
- To offset the threat of sabotage and subversive activity.
- DISI will become the education base.

By now you can see why I refer to the Institute as the academic center of the Defense Industrial Security Program. In fact, the future appears to hold an even greater role for it than that of industrial security.

Supporting the Institute's efforts are education and training staff specialists assigned to each Defense Contract Administration Services Region. These specialists will soon have greater visibility to industry. Their services are available as consultants to contractor facilities in setting up security programs, but, it doesn't end there. They are also available to give indoctrination sessions to contractor employees.

INDUSTRIAL SECURITY STAFF SPECIALIST
(Education and Training)

- Assigned each DCASR
- Available to consult
- Available to indoctrinate

In effect, we want this man to get actively into the contractor's plant on a greater scale than in the past. He will be part of the effort to ensure that the new criteria on classification management are understood and implemented.

This brings us back to the most significant change in the Defense Industrial Security Program since 1968. It was in 1968 that the DD Form 254 was revised; the present storage standards became mandatory and the procedures for processing of the Personnel Security Questionnaires changed to accommodate the privacy portion of the forms. The present emphasis on classification management is another big step in the continuing effort to bring security requirements in line with the ever changing trends of society and our national interest. I will not dwell on the details of the new program since other sessions will go into these in depth. Instead, I will alert you to some of the changes that have taken place in our operations which facilitate implementation of the classification management program.

In 1971 and 1972 a number of organizational changes took place in our operation. Previously the Offices of Industrial Security were a part of district and area offices of DCASRs. This was changed with the establishment of the Industrial Security Field offices in each of the major metropolitan areas where we have a concentration of cleared facilities. These field offices report directly to the Office of Industrial Security at the DCAS Region level. This new organization gives the regional chief direct authority over his operation, region wide. It permits better utilization of our resources and gives us a centrally controlled operation which is proving to be most effective.

ORGANIZATIONAL CHANGES

- Field offices report direct to region
- Classification Management Specialist
  - ★ Assigned to operation division
  - ★ Uniform position description
  - ★ Special training conducted

In August 1972 another change resulted in transfer of the Industrial Security Staff Specialist for classification management from the Facilities Division to the Operations Division. This change is designed to get the classification management man closer to where the action is. Essentially, we hope to achieve greater attention to classification management during industrial security inspections at the contractor's facility level. We want to bring the classification management specialist into closer contact with industry program and project managers so that classification programs can be identified and resolved as expeditiously as possible.

In order to insure a uniform understanding of the greater depth now encompassed in this function, a standard position description was furnished all regions in November 1972. The job summary portion of this position description states that the Classification Management Specialist . . . "Conducts inspections and special assistance visits at contractor facilities to evaluate the effectiveness of the specifications in actual application; provides guidance in the interpretation and application of downgrading and declassification instructions; advises and assists contractors, DCASRs and user agency activities in solving problems related to security classification."

I feel that another sentence in this position description is also important. It reads, "In coordination with the Education and Training Specialist, (he) develops and presents specialized subject matter in the area of classification management, including indoctrination, and advanced or specialized instructions in certain areas to groups of contractor and DCASR personnel." This validates my previous observation that education is important to successful implementation of requirements.

We tried something new in December 1972 by bringing together the Classification Management Specialists and the Education and Training Specialists for a three-day course of instruction on the changes to the Industrial Security Manual. During this course, which was held at the Defense Industrial Security Institute, the proposed changes were discussed in depth to permit each attendee the opportunity to thoroughly understand their intent . . . to achieve a uniformity of understanding particularly as regards Appendix II and paragraph 11b of the manual. Each region was then given the task of setting up training sessions in advance for their industrial security representatives to prepare them for the implementation of the new

requirements within industry. This training in advance should result in our people being able to offer their professional assistance to those contractors who have difficulty in implementing the changes.

SPECIAL TRAINING ON APPENDIX II ISM FOR DCASR

- Classification Management Specialist
- Industrial Security Education and Training Specialists
- Industrial Security Representatives

DCASRs Conducting Sessions for Industry

DCASRs have also been conducting a number of conferences with industry groups to afford the maximum opportunity for contractors to learn the new procedures and to ask questions on that which is not clearly understood.

We are sincere in our desire to make the Classification Management Program work. During the special training course in December we emphasized that the Classification Management Specialists are required to document those instances where cost avoidance or savings have resulted from classification management reviews. This is included in the position description to which I referred a few moments ago.

I am convinced that industry can be of great assistance in this effort by documenting these cases also and bringing them to the attention of our people in the region. This technique is not new or novel. Obviously if you can show cost avoidance or savings by the effort expended, it tends to support the value of the operation. It also results in a positive Classification Management Program.

We are still in the process of mechanizing one of the more routine aspects of classification management. Basically, we will establish a computer record in each DCASR of each Contract Security Classification Specification, the DD Form 254. While we had started this under a major DoD system of automating contract administration procedures, the major system, known as MILSCAP and MOCAS II, has been terminated. Right now we are exploring ways of continuing the mechanization of our industrial security subsystem as a "stand-alone" program. Hopefully we will get permission to put the system in operation this year.

For years we have pretty well confined our actions to notifications to the contracting activity that a 254 has not been received or that a notice of review has not been received. In one sense you might say we have been known for our "delinquency notices." Naturally this does not make the responsible activity happy.

Through our proposed mechanization we will avoid the need for a "delinquency notice" by sending out an "alert notice" 30 days before the anniversary date of the required review. This will be generated automatically by the computer. Only after 60 days have elapsed, with no notice of review received, will the "delinquency notice" or "overage report" be generated.

This use of the computer is just a small step in what eventually may expand into further adaptations of computer science to the classification management field.

There is one final item relating to classification management and industrial security that I would like to comment on.

Each of us has our own opinion of how well the new classification, downgrading and declassification criteria will work. Adjectives alone won't measure it but numbers will. Shortly after the Department of Defense implemented Executive Order 11652, we heard a number of pros and cons on how effective the new requirements would be as they affect industry. We heard such statements as, "nearly all the 254s are exempting the information from the Advanced or the General Declassification Schedule." This could be true as regards specific contracts but certainly this would not hold true across the board.

To get to the facts, each of our 11 regions conducted a check of all prime contract 254s received during February and March 1973. We wanted to know how many of these were exempting classified information from the ADS or GDS. We also were interested in how many of these exempting were using category 3 as their justification.

The results of this study were enlightening. A total of 1,758 prime contract DD Forms 254 were looked at in these two months. Sixty-one percent of these, either in whole or in part, exempted classified information from the GDS. Of that number 75 percent listed category 3 as their reason for exemption. Another finding showed that 6 percent of the DD Forms 254 reviewed contained instructions in conflict with the requirements of DoD Regulation 5200.1-R.

ANALYSIS OF CONTRACT SECURITY CLASSIFICATION SPECIFICATIONS
(DD Forms 254)

Feb–Mar 73 = 1,758 Prime contract DD Forms 254 reviewed

61% Exempted info from GDS (whole or part)
(75% listed category 3 as reason for exemption)

6% Issued instruction in conflict with DoD 5200.1-R

Baseline for Future Comparisons

A number of other breakouts were possible from this study and the entire package was furnished to the Deputy Assistant Secretary of Defense (Security Policy).

At present, these percentages give us a baseline for further comparisons. Whether 61 percent is high or low we cannot really say. Those of you who thought that "nearly all," or the "vast majority" of DD Forms 254 were exempting classified information may feel the figure is low. Others who were hoping for more use of the ADS and GDS probably feel the figure is high.

Perhaps the most significant feature of these numbers is their future value to determine whether there is increase or decrease in use of the exemption criteria.

In this presentation I have highlighted those industrial security administration policies which could be labelled new, although I prefer to think of them as improvements.

We look to the Defense Industrial Security Institute as a new identity with potential expansion of its curriculum. . . . The new mission assignments of industrial defense and the proposed Information Security Management Course would certainly indicate this will be the case.

The direct line control now exercised over all field operations in the DCASR by the Regional Office of

Industrial Security Chief serves to place the effort where the need may be the greatest.

Greater visibility can be expected of the Education and Training Specialist and the Classification Management Specialist in each of the 11 DCASRs. They will actively get into contractor facilities where their services can be of assistance. The transfer of the Classification Management Specialist to the direct control of the Operations Division Chief assures closer relationships on the day-to-day contacts.

The mechanization system we are planning to set up to send out alert notices when reviews of DD Forms 254 are due should result in more attention being given to the review requirements. Additionally, more effort by our people will be expended on substantive reviews of these 254s in conjunction with visits to contractor facilities.

Finally, I feel certain that a cooperative effort between the facility Security Supervisor and our Industrial Security Representative will result in meeting all of the major objectives of Executive Order 11652.

The end result will be to better safeguard that which truly needs protection against unauthorized disclosure. ■

A STUDY OF THE EFFECTS OF SECURITY CLASSIFICATION RESTRICTIONS ON TECHNICAL COMMUNICATION

Major Robert L. Taylor,* USAF,
Doctor of Business Administration,
Department of Economics and Management,
U.S. Air Force Academy

Security classification of scientific and technical information is a serious concern of many engineers and scientists. Two major arguments have developed. On the one side are those who believe that any restrictions on information impede the nation's scientific and technological progress. On the other side are those who believe that military restrictions are necessary and that scientific and technical progress continues in spite of secrecy. Neither side offers substantive proof.

I. SECURITY CLASSIFICATION IN SCIENCE AND TECHNOLOGY

Past investigations of security restrictions have been lacking any empirical support. Little factual evidence has been gathered. In short, there is a problem of method. To see this problem clearly, the reader will need to know something about the theory of information restriction.

Theoretical Elements of Security Classification in Science and Technology

The withholding of information is an aspect of power; and it has a long history. Most often, secrecy has been associated with military and political objectives. The imposition of secrecy upon scientific and technical information is a recent phenomenon, traced most often to the developments in weaponry during the Second World War. As the Committee on Government Security [18] noted:

> From the beginning there has been universal acceptance of the fact that vital military information must be protected from unauthorized disclosure. There has likewise been general acceptance that diplomatic negotiations and correspondence should be subject to restrictions on its availability. The third category, neither military nor diplomatic matters, but that which is currently described as "the public's business," is the area over which the most controversy has taken place. The most trenchant proof of this is the fact that relatively little has ever been written against the right, and indeed, necessity to classify military or diplomatic information while volumes have been filled with argument for the right to all access to information about the "public's business." The basic difficulty, however, lies in defining the scope of the latter category.

Scientific and technical information appears to belong to the first and third categories.

Technological lead time is most often given as the reason for restricting the dissemination of scientific and technical information. For example, the Export Administration Act of 1969 is designed to "restrict the export of goods and technology which would make a significant contribution to the military potential of any nation or nations which would prove detrimental to the national security of the United States." [9] Thus, scientific and technical advances that can be linked to military threats and capabilities are subject to dissemination restrictions. It is assumed that potential enemies will eventually duplicate our side's scientific and technical achievements and that we can keep one step ahead—maintain technological superiority—by delaying the enemy.

But the intent, however sound in theory, is hampered by its implementation. Decisions to restrict information are made at the highest levels, but they must be interpreted in the research-and-development laboratory by individual scientists and engineers. Thus, for example, the high-level decision to classify the maximum speed of a new aircraft may lead to the lower-level decision that the material composition of the leading edge of the airfoil must also be classified, inasmuch as the latter information could reveal potential stress characteristics and, therefore, the maximum speed of the aircraft. Consequently, a breakthrough in materials technology could be stifled. Persons who are aware of this sort of thing say that lack of clarity in classification guidance, over-classification (to be "safe"), and administrative difficulties in complying with classification policy are the reasons why the present security classification system is not effective.

Is this an adquate explanation? Or does the problem go deeper than that? Examination of the arguments is necessary before any conclusions can be drawn.

Security Classification—A Barrier to Information Dissemination

The argument against security classification in science and technology is essentially one of opposing any barrier to the free exchange of information and ideas, which is so

*The views expressed herein are those of the author and do not necessarily reflect the views of the United States Air Force or the Department of Defense.

often considered a vital part of the scientific process [11]. The need for free exchange is associated most often with the validation of research: according to The National Academy of Sciences, "The process of discovery is not complete until the knowledge of all peers has been brought to bear on the assertions and no flaws have been found in the light of present knowledge." [7]

Evidence that security classification has actually impeded scientific and technical advance in sparse. In 1959, 19 American Nobel Prize winners testified to delays in scientific and technical discovery because of restrictions [13]; specific instances were cited. Since that time, a number of Executive and Congressional committees have examined the problem; for a review see [14]. In general, the investigators have concluded that Department of Defense procedures have impeded scientific and technical advance because of excessive classification restrictions.

Perhaps the most outspoken criticism came during the U.S. Senate hearings on the antiballistic missile [15]. A number of witnesses opposed any further restrictions on scientific and technical information. Many believed that the nation's scientific and technical capabilities were not being used to capacity because of duplication of effort, the refusal of young researchers to work on classified projects, undefined "invisible colleges" of classified researchers, and the unwillingness to develop nonmilitary applications of important scientific and technical discoveries.

An interesting argument against restrictions is this: by marking information for protection we identify critical information for the enemy, who then concentrates his research in the "blanked-out" field. A completely open scientific and technical information network might make such enemy searches so complex as to limit the amount of information he could gain. At the same time, our own research would not suffer. Support of this argument comes from U.S. developments in computers and nuclear weapons. Discoveries and developments in computer technology have been open and widely disseminated, while the tightest of security restrictions have been applied in nuclear weaponry. Yet the United States is the world's leader in computer technology, and a number of nations have managed, despite U.S. secrecy, to develop a nuclear weapons capability.

An outspoken opponent of information restrictions is Edward Teller. In recent years he has proposed the declassification of all scientific and technical information [15]. Perhaps a more balanced argument is provided by H. L. Wilensky [17], who recognizes that the lead time over our adversaries is extended to our own scientists. Wilensky would even suggest that our enemies get our scientific and technical information long before our own scientists and engineers.

However, even the strongest critics of security classification in science and technology will admit that there can be military requirements for secrecy. The problem, as they see it, is to draw a sensible line between scientific and technical achievement, which requires openness, and military policy, in which secrecy is sometimes imperative. A concerned organization has put it this way:

> There is a deep and continuing conflict in U.S. policy between the need for greater public dissemination and the equally pressing need for official secrecy. Any attempt toward resolution of these diametrically opposed policies undoubtedly would involve achieving a consensus. [4]

Security Classification—No Effect on the Advancement of Science and Technology

Let us turn now to the antithetical position. Here, the logical arguments support the view that science and technology can progress successfully in spite of security classification restrictions.

The first argument is that secrecy is just another form of privacy. The free enterprise system has developed elaborate industrial security restrictions under the guise of proprietary information. Scientists acknowledge the value of such restrictions. A writer in *Science* asserts: "privacy is also necessary for the protection of the early stages of pure research in situations in which the highly competitive nature of modern science makes the research worker wary of premature disclosure." [11] In a sense, we can consider the United States to be "in competition" with adversary nations, and therefore to have a "proprietary" interest in scientific and technical information. Writers in support of this argument cite the apparent Soviet successes in science and technology under conditions of secrecy [13]. However, this view can be questioned on two points: (1) The Soviet political and social system is quite unlike ours; and (2) centralization of Soviet research and development may be such as to permit a thorough internal information exchange while limiting dissemination outside the scientific and technical community.

The second argument is that no real evidence exists that scientific and technical achievement has been denied because of secrecy. The Committee on Science in the Promotion of Human Welfare (American Association for the Advancement of Science) searched the literature and interviewed persons concerned with secrecy and science; and the committee found little evidence that secrecy had inhibited basic research [11]. The physicist and novelist C. P. Snow, in his account of the effects of secrecy on the scientific and technical impetus in Britain during World War II, says:

> Again unfortunately, the constraints of secrecy, though they disturb the judgment, do not disturb the scientific process. . . . Science needs discussion, yes; it needs the criticism of other scientists; but that can be made to exist in most secret projects. Scientists have worked, apparently happily, and certainly effectively, in conditions which would have been thought the negation of science by the great free-minded practitioners. But the secret, the closed, the climate which to earlier scientists would have been morally intolerable, soon becomes easy to tolerate. I even doubt whether, if one could compare the rate of advance in one of those which is still open to the world, there would be any significant difference. It is a pity. [12]

What is the Problem?

These arguments, pro and con, are continually stated and restated—in the press, in scholarly journals, and in private conversation. The arguments are as emotional as they are logical—and the emotional side has prevailed in the few attempts to gather empirical evidence. Clearly the debate has not helped us to determine the true effects of

security restrictions in science and technology.

The historian Arthur Schlesinger, Jr. [10], quotes a Congressional subcommittee witness—a "retired Pentagon security officer"—as stating that at least 99.5 percent of the classified documents then extant could not possibly have been prejudicial to the defense interest of the nation [16; I:104]. Could any one person have the military background or the technical knowledge to make such a statement? This is an excellent example of the sensational assertions that get publicity while real evidence is neglected or ignored.

II. COMMUNICATION IN RESEARCH AND DEVELOPMENT

Information dissemination is an integral part of the research and development process. Science and technology require constant interaction of colleagues and predecessors [8; p. 7]. Studies have identified the major role played by interpersonal communication in the dissemination of information [7; p. 73]. Careful research into the nature of such exchanges has produced several guidelines.

A keystone work is that of T. J. Allen [1] of the Massachusetts Institute of Technology. He defined a two-step flow process in scientific and technical communication. He found that information from outside the research-and-development laboratory flowed through mediators ("technological gatekeepers") to the scientific and technical users within the laboratory. By identifying technical discussion choices within the laboratory, Allen was able to identify the engineers who were the "stars" of the discussions. He found that the stars were seen by their colleagues as the sources of the best technical ideas in the laboratory. Further investigation showed that the stars had a greater number of information contacts outside the laboratory than did their colleagues: they attended more professional meetings, published more technical papers, and saw more vendors and customers. They were the technological gatekeepers who mediated the flow of scientific and technical information into the laboratory.

Using analytical procedures developed by Allen and others [2] [5] [6], I collected data from 184 engineers at a large, military "inhouse" research-and-development laboratory (hereinafter called "the laboratory" or "the lab"). A questionnaire was combined with personal interviews to study the social relationships and demographic characteristics of the respondents and the patterns of technical communication at the laboratory.

Gatekeepers were identified by their internal and external communication attributes. Internal attributes were defined by the number of times the engineer was chosen for technical discussion by his colleagues and the number of times he was chosen as a source of technical ideas. External attributes were defined by the number of the engineer's communication contacts outside the laboratory. Those engineers who ranked high in both attributes were defined as technological gatekeepers. Twenty-four engineers fitted this role. The gatekeeper identifications were confirmed by colleagues and supervisors.

My findings differed in some respect from those of previous studies. I found that (1) the external communication needs of military in-house researchers were mitigated greatly by the infusion of technical information into the laboratory; (2) gatekeepers were differentiated by topic, and not the media monitored; and (3) the gatekeeper role is implicitly recognized by the engineers even though its development may be spontaneous. I had to conclude (among other things) that the formal media do not meet the information needs of engineers—or, conversely, that engineers are not adequately trained in the use of the formal information sources. In either case, the technological gatekeeper's role appears to be a natural response to an information need.

A Two-Step Flow Process for Security Classified Information?

My investigation confirmed, at least in essentials, the existence of the two-step flow process and the role of the mediator. The logical question to ask next was this: What characteristics of security classification restrictions might mitigate the flow of information? My investigation indicated that both the internal and the external communication characteristics of information flow in the laboratory were affected. The investigation proceeded in keeping with two main observations:

1. Technical discussion partners must be able to demonstrate a "need to know" the classified data. And, since conferences must be conducted in secure areas, informal discussion (at lunch or out of the lab) is severely restricted. Thus, technical discussion and the sharing of technical ideas is confined to as small a group as the classified project demands—by choice as well as design.
2. The choice of external media is quite limited. There are classified technical reports in a number of fields. Any researcher having the proper clearance and a need to know can obtain a copy of a classified report; but first he must know that the report exists. Classified technical reports are indexed; but researchers working in unclassified areas are not able to obtain information abstracted from the classified documents. Dissemination of classified indexes is quite limited; therefore, browsing for materials is nearly eliminated. The control of classified information inhibits the researcher from requesting more than he needs to know; yet abstracts and titles are often deceptive with regard to the actual contents. Finally, telephone conversations and other informal technical contacts outside the lab are prohibited.

Information produced at the laboratory, too, can be restricted. This is a "Catch 22" for the investigator: only by evaluating the technical information produced at the lab can he determine the extent of security classificaation restrictions—and the possibility of the evaluation is denied to him. And, of course, the investigator's knowledge of the nature of any dissemination restrictions can be of importance in making statements about the effectiveness of the technical information flow.

The research-and-development laboratory is ideal for studying the effects of security classification restrictions. Both the sources and the users of information are represented, and this permits data to be gathered about the full cycle of the security classified information flow. There is reason to believe that the two-step flow process model does not apply for security classified information.

We can also speculate, from evidence advanced by Tanguy [12] and others, that a significant amount of scientific and technical information generated at the lab will be restricted as to its dissemination.

Hypotheses

In the light of the preceding observations and conjecture, three hypotheses were proposed:

H.1 A two-step flow process for security classified information will not be identified.

H.2 There will not be a significant differences in ranking of security classified sources by the users of classified scientific and technical information.

H.3 A significant number of laboratory-generated documents will be subject to prohibition of open publication and diffusion, yet not subject to security classification restrictions.

III. ANALYSIS AND DISCUSSION

During the interview phase of the research, each engineer was asked about his experience with security-classified information. The five questions asked are presented in Table I. Fourteen respondents reported significant contact with and use of classified technical information. Interviews with librarians, information specialists, and security managers provided collateral data.

TABLE I

INTERVIEW QUESTIONS AND SUMMARY DATA

1. Approximately what percentage of your research time do you work with security classified information? (n = 184)

0–20%	21–40%	41–60%	61–80%	81–100%
149	21	0	6	8

2. In your opinion, have security classification restrictions seriously impeded the flow of scientific and technical communication in your specialty? (n = 184)

Yes	No
58	126

3. Do you receive abstracts of classified technical information in your specialty? (Asked only of the 14 respondents who indicated 41 percent or more in Question 1.)

Yes	No
0	14

4. With whom in your work group would you consult for the latest security classified technical information relevant to your current project? (n = 14)

   Number of respondents naming no individuals = 14

5. In searching for classified technical information, to which sources (in order) do you normally turn? (n = 14)

   (Data presented in Table II)

Security Classified Information—No Information Flow Defined

The respondents indicated that they did not discuss security-classified technical information with their colleagues. They were unanimous in saying that the search for security-classified scientific and technical information was an individual responsibility. As shown in Table I, no one named a colleague who might have a greater number of external links to security classified information. Furthermore, many of the respondents felt that classified discussions were kept to a minimum and were carefully circumscribed by information needs.

In general, the engineers felt that they did act differently when searching for security classified information. Each had a procedure, and all believed that they were able to obtain the information needed. None could actually verify the thoroughness of his information-gathering efforts, but the office files did contain security classified technical reports from a number of Governmental agencies and defense contractors.

The Defense Documentation Center (DDC) lists certain classified reports in the technical areas of interest to the lab group. Engineers admitted that information might exist elsewhere; but, generally, they were confident that all useful information had been identified and was available from the DDC. Typical comments of the engineers were:

> I feel confident that all the information in this area is in my files, but don't ask me to prove it.
>
> Really, anyone working in this area would consult us and so I have no need to look outside—all the information eventually comes here anyway.
>
> No one else is interested in this topic except us. At least, I don't think so.

Clearly, no two-step model of information-gathering could apply. Each engineer appeared to act independently in his search for classified technical information. The next step was to define the independent actions.

Table II represents the results of asking each respondent *his* priority for security classified technical information sources. The data indicate that the internal files and library sources were used first. This finding agrees with studies, cited earlier, indicating that engineers will turn first to the most accessible information sources.

TABLE II

RANKING OF CLASSIFIED TECHNICAL INFORMATION SOURCES

Classified Technical Information Source	Number of Professionals Using Source			
	First	Second	Third	Fourth
Office classified files	14	0	0	0
Library and technical information office	0	10	4	0
Contract bibliographies	0	4	8	2
Defense Documentation Center abstract lists	0	0	2	12

Kendall Coefficient of Concordance (W) = .57.

One would expect the literature to be the major source of security-classified technical information. Indeed, the engineers in the lab turned to the literature for a large

proportion of their information needs. Thus, we can conclude that the restrictions associated with security classification confined these engineers to a source not normally used in information-gathering by other engineers. Unfortunately, we cannot assess the *qualitative* effectiveness of the information-gathering. If, however, the literature and other formal media are inadequate for scientific and technical information in general—an inadequacy that creates the technological gatekeeper phenomenon—it is improbable that the formal sources are adquate for the security-classified elements of the technical information flow.

In summary, a two-step flow process for security-classified scientific and technical information was not identified; so hypothesis H.1 is confirmed. In addition, there was not a significant differences in rankings of security-classified sources by the users of classified scientific and technical information; so hypothesis H.2 is confirmed.

The Dissemination of Laboratory Generated Technical Information

The laboratory publishes yearly an index of the technical reports generated. Table III shows the extent of dissemination restrictions that were applied in 1970. In that year, 193 reports were published. No security classification restrictions were applied. However, 127 documents (65 percent) were limited in their distribution to U.S. Government agencies. From this data, it would appear that the technical information generated by the lab is severely restricted.

TABLE III

DISSEMINATION STATISTICS FOR LABORATORY DOCUMENTS

	Number of Laboratory Documents Generated in 1970
Classified:	
Top Secret	0
Secret	0
Confidential	0
Unclassified:	
Limited distribution	127
No restrictions	66
Total	193

However, another report provides a clearer picture. Table IV is an exact copy of the report (minus identifying information). It records the requests for information directed to the laboratory from the general public. Of 347 requests, none was denied. Unclassified documents with limitation statements were referred to the originator for approval and, in *all* cases, the requests were granted. The appropriate security offices verified the "need to know" of the persons requesting classified documents; and, again, all requests were granted.

Two notes are necessary. First, nothing is known about how many interested readers of the technical-report list failed to request a report because they did not believe they could obtain a report that was unclassified but limited. Second, no indication was given as to the dissemination of the technical-report list itself. (A great many of the documents were, however, indexed by the Defense Documentation Center.)

TABLE IV

REQUEST FOR INFORMATION FROM THE GENERAL PUBLIC*
"Freedom of Information"
(For period 1 May–1 Nov 71)

Number of requests for technical information from the general public		347
Disposition of requests:		
Requests referred to other military organizations because of incorrect address	16	
Foreign requests	35	
General public (unlimited distribution) requests referred to Defense Documentation Center	160	
General public (limited distribution) requests released by originator	94	
DoD contractors (security classified) requests released through the appropriate security agency	42	
Total		347

Note: No denials for information during above period.
**Information taken directly from lab report.*

The combined data in Tables III and IV show that, insofar as was possible, the laboratory's technical output was given wide dissemination. However, no record exists as to the restricting of information dissemination to interested requestors. Also, a significant number of laboratory-generated documents were subject to dissemination restrictions that appeared to prohibit dissemination. Hypothesis H.3 is, in essence, neither proved nor disproved.

Security Classification Management

The laboratory seemed oriented to security classification management. For example, researchers said that all classified information referred to in an unclassified technical report was separated in an appendix. The engineers believed that the guidance provided them was thorough: whenever information about military threats was combined with information about military capabilities, the information was subject to security classification. A number of respondents remarked that security-classification decisions were reached by consensus: no one person made classification decisions, and the process was continually reviewed.

Interestingly, the guidance given reflects this, as is shown in Table V. In a comparison of classified guidance statements, the lab procedures are shown alongside the guidance used at another lab. Although the latter appears more defined, it presents great difficulties in interpretation. Should everything associated with maneuverability be classified, such as the throttle control? To be on the safe side, one would be able to justify a number of classification decisions that are only remotely related to maneuverability.

On the other hand, the guidance used at the subject

TABLE V

COMPARISON OF SECURITY CLASSIFICATION GUIDELINES

Typical Subject Laboratory Guidance*

The work and developed data under this project and supporting tasks are generally Unclassified. However, new techniques which constitute a breakthrough in current state-of-the-art and have military application will warrant protection up to and including the Secret level. Decisions as to warranted level of classification to be assigned will be made by [laboratory project group].

Typical Comparison Laboratory Guidance*

Specific performance	Secret	Applies to speed, altitude maximum and minimum range, maneuverability limitations, and other specific performance parameters.
General performance	Confidential	Applies to parameters not within scope of above. Performance when no figures are used is Unclassified.
Physical characteristics	Unclassified	Applies to length, height, weight, scale models, and photographs.
Estimates or proven conclusions as to system capabilities and/or operational limitations	Secret	
Vulnerability	Secret	Applies to any data relating to overall system vulnerability.

**Taken directly from security classification guides. Only 5 of nearly 40 items for comparison laboratory project reproduced.*

lab demanded a consensus as well as an explicit justification. Further, a review board had to validate the decision; in effect, the board made a second judgment. Altogether, there was a conscious effort to keep as much information unclassified as possible.

IV. IMPLICATIONS FOR FUTURE RESEARCH

How does all this compare with the assertion, by opponents of security classification, that technological advance has been nearly halted because of secrecy restrictions? I believe my data shows that this was not the case in this laboratory. However, it must be admitted that the present study has its limitations--notably the absence of validating data. This is because the design of the study did not provide for a detailed qualitative analysis. The primary purpose of the study was to define a method and to ascertain the feasibility of further study. If this laboratory is typical of the security classified research and development environment, some meaningful directions for continuing study have been identified.

First, the present study must be replicated. The security environment encountered was such as to indicate that either this lab has a unique and effective security program or the magnitude of dissemination problems needs to be reevaluated. In any case, the present method needs to be extended to include validating procedures. To this end, a second study should include a parallel project. A technical evaluation team would be charged with identifying two technical achievements of equal importance. One would be classified; the other would not. Records of the dissemination of the information, of when engineers heard of the achievement, and of adoption or application of the achievement would then be gathered over a period of time. Measuring the time lags between the discovery and the dissemination saturation points would indicate probable effects of security classification restrictions.

The present research showed that engineers in one large research-and-development laboratory believed that their search for, and accumulation of information under security classifications was as effective as their efforts in unclassified areas. Yet, the literature is not generally recognized as being effective. At the same time, it appears that laboratory-generated information was given wide dissemination. Since gaps are apparent in both sets of findings, the research program outlined above should assist in more clearly defining the impact of security-classification restrictions on the flow of scientific and technical information.

V CONCLUSIONS

1. There does not appear to be a two-step flow process model for security-classified scientific and technical information. Instead, information search approximates a unidirectional model, with the literature being the only important information source.

2. Because the source consistently cited by engineers for security-classified information was a source least often used in unclassified searches, there is reason to believe that the effectiveness and efficiency of information-gathering is seriously impeded. There is however, no empirical proof that this is the case.

3. Laboratory-generated information was generally subject to dissemination restrictions, but rarely because of security classifications. Actual dissemination of information was aimed toward meeting the needs of all eligible requestors.

4. A positive attitude toward security can be instilled among technical personnel. This significantly influenced the laboratory engineers to apply security classifications that strongly supported the use and dissemination of information.

5. Continuing research studies are needed to define more specifically the impact of security classification restrictions on the flow of scientific and technical information.

REFERENCES

[1] Allen, T. J. "Managing the Flow of Scientific and Technoiogical Information." Unpublished Ph.D. dissertation, Massachusetts Institute of Technology, 1966.

[2] Allen, T. J. and Cohen, S. I. "Information Flow in Two R&D Laboratories," *Administrative Science Quarterly,* vol. 14, pp. 12-19, 1969.

[3] American Association for the Advancement of Science. "Strengthening the Basis of National Security," *Science,* vol. 120, pp 957-959, 1954.

[4] "Dissemination and Technological Progress," Panel discussion at the Fifth National Seminar of the National Classification Management Society, Washington, D.C., July 22-24, 1969.

[5] Farris, G. F. "Executive Decision-Making in Organizations: Identifying the Key Man and Managing the Process." Cambridge, Mass.: Massachusetts Institute of Technology Sloan School of Management Working Paper 551-71, 1971.

[6] Frost, P. and Whitley, R. "Communication Patterns in a Research Laboratory," *R&D Management,* vol. 1, no. 2, pp. 71-79, 1971.

[7] National Academy of Sciences, "Scientific and Technical Communication: A Pressing National Problem and Recommendations for Its Solution," Publication 1707, Washington, D.C., 1969.

[8] President's Science Advisory Committee, *Science, Government, and Information. The Responsibilities of the Community and the Government in the Transfer of Information.* Washington, D.C.: Government Printing Office, 1963.

[9] Public Law 91-184, "Export Administration Act of 1969."

[10] Schlesinger, A., Jr. "The Secrecy Dilemma," *The New York Times Magazine,* February 6, 1972, pp. 12-13 and 38-50.

[11] "Secrecy and Dissemination in Science and Technology," *Science,* vol. 163, pp. 787-790, 1969.

[12] Snow, C. P. "Science and Government," *Science and Technology,* no. 85, pp. 31-46, 1969.

[13] Tanguy, R. B. "The Impact on National Security Caused by Restrictions on Defense Research and Development Information," *Classification Management,* vol. VII, pp. 144-146, 1971.

[14] Taylor, R. L. "Secrecy and the Dissemination of Scientific Information," *Industrial Security,* vol. 5, pp. 4-17, 1971.

[15] Teller, E. "Problems of Secrecy," *Journal* of the National Classification Management Society, vol. 6, pp. 136-143, 1971.

[16] U.S. Government Information Policies and Practices—"The Pentagon Papers," Hearings before a subcommittee on the Committee on Government Operations, 92nd Congress, June 23-25, 1971.

[17] Wilensky, H. L. *Organizational Intelligence.* New York: Basic Books, 1967.

[18] Wright, L. "Document Classification Program," Committee on Government Security: Report Presented to the U.S. Congress, Washington, D.C.: Government Printing Office, June 12, 1957, pp. 152-313. ■

OUR CREDIBILITY GAP IS SHOWING

Mr. Dean Richardson,
NCMS Director (Texas Instruments)

What I am about to say to you today may sound like heresy--heresy, that is, by the creed of a responsible company security officer or his opposite number in the oligarchy that many people call the military-industry complex. As a responsible security officer I don't endorse some of the things that I predict are going to happen; I don't pretend to admit that I know all of the things that are going to happen, but I'm warning you today that unless we get some practical approaches in handling our classified material, we're going to lose control. After all, the success of our program depends upon the individuals who are handling classified information and their knowledge, ability and motivation to properly handle this material. Ellsberg took it upon himself to decide that the classified documents he released to the press were not classified. In his own mind and conscience he was not doing anything wrong. He felt, we understand honestly, as a responsible U.S. citizen, that the public should know about what was going on. Now I don't endorse what Ellsberg did, but I'm telling you that what he did is a manifestation of what's happening in the minds of intelligent individuals; and remember, he successfully challenged our security rules.

We are not dealing with robots—the rules that are made for industry to follow have got to consider that the individuals who have to follow these rules are intelligent; often times a lot more perceptive than those of us that make the rules. Accordingly, a regulatory body must be more than careful to ensure that the rules made are not impractical and that they are practiced in the same way by all the people dealing together. Double standards, one for industry and one for Government, should not exist because people in industry are dealing daily with people in Government. These things seem to be lost sight of when rules are being made. It must be recognized that the needs of Government dictate the needs of industry; in order to do the job that the Government wants done, industry must respond in a timely, efficient manner. Industry cannot have efficiency and timeliness if their

method of operation is governed by impractical regulations—regulations that do not meet the needs of our national defense.

Now what I'm leading up to is just this, there have been lots of changes over the past two years. I see a creeping paralysis and a suffocating over-control being imposed upon industry by our opposite numbers in the Department of Defense—this control apparently stems from fear or ignorance and let me explain this. *Fear* that the people that they are dealing with are robots, unintelligent individuals, unable to cope with situations which would arise in the protection of this material. *Ignorance*—well, some of the things that are appearing in the Industrial Security Letters indicate a total lack of appreciation for the security officer's position in industry, the intelligence of the engineers and scientists with whom he deals, and a lack of understanding of the rapport, or lack thereof, and the interplay that exists between the Government customer and industry contractor.

Now I'm not critizing any one person, any one group of people, but what I am saying is that we have got to sit back, have a re-look; sit down with the people with whom we are dealing and discuss things with them rationally and maturely. We must recognize the potential danger of over-control and impracticality of some of the rules being promulgated. Let me give you just a few examples of the impracticalities that are an affront to the intelligent scientist, engineer or technician.

Most companies have gone into a detailed, intensive education program to explain the President's Executive Order 11652 and the reasons for change. Most of the people with whom we work are familiar with existing regulations and carry them out willingly, because they are practical—unfortunately their reaction to the Executive Order is, "Why change again, we're just getting used to this system; we just know now how things are going." So you see, it takes a pretty intensive education and motivation program to encourage these intelligent, practical people to willingly follow the new rules. Therefore, we encourage them and explain to them why the President wanted to change the security downgrading and declassification markings, and they say, "well, okay, that sounds like a pretty good idea; maybe it's going to make sense,"—then we start receiving DD 254s that have been remarked. Now, there is nothing uniform about these DD 254s except uniformity by specific User Agency. For example, one User Agency appears to have taken the position that most of the material should fall in the GDS category; another agency has been forced, I understand, by their legal office to develop two new classification markings involving the term "Excluded." This agency also appears to believe that most of their material must be exempt for 30 years, since most of the DD 254s from that agency are coming in with the declassification date in the next century, such as, 2009. A third User Agency appears to have mixed attitudes toward markings, however, the majority of that User Agency's Security Guides are marked Exempt with an indefinite declassification date. My quote for the year is a quote made by a gentleman from this agency who during discussions as to how we should mark a proposal document asked, "What category does the material fall under?" Our reply was that it would probably fall under the new Exempt Category 3, and he said, "Oh yes, that's exempt, that means automatic exemption for 30 years." So you see, gentlemen and ladies, even the people that make the rules don't fully appreciate the implications or the reasons for the new rules and they don't seem to make an attempt to carry out the intent of the President's Executive Order.

Now, let us look at another problem—impractical application of a theoretical truism, and this concerns the directives contained in the recent Industrial Security Letter 73L-3. Over a year ago, some airline companies instituted on-board-baggage checks at major airports. At this time I asked for a DoD position, particularly concerning plans for clearing handcarried material through the airport checkpoints—a year later, ISL 73L-3, in some detail, answered my questions, and I'm sorry I asked. However, in the meantime all of us in industry and most of you in the Government shifted gears and effectively dealt with the airlines and with the FAA in ordar to preserve the integrity of the material that occasionally our people have to handcarry to meet *deadlines* or *customer demands*. Now, I want to emphasize those last important words—*Deadlines* or *Customer Demands*—because there seems to be a profound opinion in the minds of some of our Industrial Security authorities that industry types, willy-nilly, hand carry classified material because they want to. Gentlemen and ladies, I can tell you for a fact that that is an absolute and total fallacy—a sophism. Being burdened by needing to carry classified material is about the worst thing that can happen to a traveler. No one wants to do it. The only reason that anybody in industry ever carries classified material is because they have got to meet a deadline date in order to win or compete in a contract or satisfy a contract commitment and that's what the game is all about—winning contracts, satisfying the customer, paying your people, making a profit, increasing your standard of living. As to the other point, customers are very demanding—particularly customer's who haven't paid their bill. When our customer says fix that piece of gear or get me that report tomorrow, we fix the gear and we get the report tomorrow regardless of what the obstacles are. The material involved is protected and there's no compromise. The point here is that nobody wants to handle classified material outside the plant, and if you people who are making these rules would realize this, you'd understand that we in industry are not stupid, we do not intend to compromise any of this material because it's our livelihood also. We too are citizens of this country who believe in protecting information that the Government says is classified, irrespective of Ellsberg *et. al.*

Now, getting back to 73L-3—for the past year all of us have developed means of dealing with the FAA and the airlines. We intend to continue to deal with them in the same manner as we have in the past. 73L-3 tells us how we must handle our classified material, and that we can't carry any packages without a cognizant security office approval. How do you get the cognizant security office approval in such emergency situations that warrant handcarrying? Consider a typical situation. A customer calls on Friday afternoon, his gear is down and he wants it up immediately to meet an operational requirement. We respond! We get the material ready and it goes out Saturday, maybe Saturday night maybe Sunday or Sunday

night. How do we get DCASR's approval? This ISL also says that we must document the fact that handcarrying classified material is an absolute requirement. Gentlemen, I have said before, nobody wants to carry it, it's only carried *when it is a requirement.*

Up to now I've been talking about our contractor/customer relationship, but remember, the Defense/Industry team relationship is much closer. On numerous occasions our company presidents are called upon by one of the Cabinet Secretaries or the JCS or even the White House to brief on a problem of immediate need. These high level briefing requirements usually involve last minute timing, often over the weekend and usually involve Secret information—we may also be required to demonstrate a piece of sophisticated hardware—Do you really think that the local DCASR is going to be available during non-working hours? Could DCASR really provide any additional security protection if they were on duty?

What I am saying is that you have taken supervisory authority out of the hands of the company security officer and you are trying to run our business from a Government office that doesn't understand the interrelationships between the company, and company procedures, and the User Agency-company association. I say, back off, tell us what your requirements are, but don't tie our hands to keep us from doing business; which brings me to another impractical regulation imposed upon industry and that is—restricting the use of REA Air Express for handling Secret material. After having used this procedure for some 20 years such restriction doesn't make sense and we can't convince the scientists, engineers that it makes sense. On one hand you say ship it by carrier and on the other hand you say you can't ship it by carrier, you've got to hand carry it and then you say you can't hand carry it. All I say is, make up your minds, but in the meantime business goes on as usual and deadlines have to be met. If the deadline means that the material has got to be hand carried, this probably means a late night flight, which means late arrival or early morning arrival. The ISL 73L-3 says our courier has got to turn it over to a cleared facility or Government office. Now, where is he going to find a facility or Government office to accept material at 2:00 a.m.?

I can tell you what's going to happen. People are going to take material out of the plant without telling us—maybe unmarked in their suitcases intending to mark the material at their destination, deliver it to the customer and come home. Are they going to get caught? Not likely. But they will, eventually, they always do, somebody eventually makes a mistake. But in the meantime the worst thing that would happen is that the majority have beaten the system, and that's what we don't want people to try to do. Another thing they are going to do is to send material by REA Air Express and when they get caught they'll take their lumps. They got that proposal there in order to meet a deadline date and they probably got the contract. I can only say one thing and that is an old truism, "don't make impractical rules and above all don't make rules you can't enforce."

Gentlemen and ladies we have got to sit back, readjust our thinking, appreciate the fact that industry, security-wise, has matured. We are no infants, we are not ignorant, we do know the rules, but we are and must be practical people.

Security must make sense to the individuals who handle the bulk of our classified material and support the needs of the defense establishment. We can't go on thinking that we rule makers are omniscient. The old axiom, "Ours is not to reason why" no longer applies. Secrecy and classification of information and its handling has been exposed to the public, probably in much more detail and in depth than ever before in history. When this exposure occurs, one can no longer sit back making rules that don't make sense without answering to somebody. In the past, many impractical rules were accepted because there was something mysterious about security and classification—well, there's nothing mysterious about it now. The Pentagon Papers episode has certainly taken off all the wraps and has shown that our security system can be challenged—the Watergate incident has horrified many who at one time believed in the mystery of Secret clandestine operations.

Ladies and gentleman, we have got to return to normalcy, to a rational approach to protecting our assets. We have got to stop overreacting, we have got to recognize the intelligence of the people we are dealing with, in short, we have got to regain the credibility and the integrity that our Defense Industrial Security Program deserves. ■

CONGRESS LOOKS AT E.O. 11652

Mr. William G. Phillips,
Staff Director, Foreign Operations and Government Information Subcommittee, House Committee on Government Operations

Mr. Al Friendly, Jr.,
Staff Member, Intergovernmental Relations Subcommittee, Senate Committee on Government Operations

Dr. Earl Callen,
Professor of Physics,
American University

Mr. Phillips: I will try to summarize very briefly the history of the Congressional involvement in the classification system and then turn over the moderating task to Al Friendly when I must leave.

I think for the record we probably should state what I guess all of us would agree is a truism in this whole area. From the earliest period of our republic, the President and other Executive Branch officials have limited the dissemination of information affecting defense and foreign policy interests. Few would ever argue that our Government should not have such powers to safeguard vital military and foreign policy secrets.

It is likewise obvious that in a representative system our citizens must be informed to the maximum extent possible of defense and foreign commitments made by their Government so as to make sound electoral judgments in the selection of public officials.

The classic dilemma is thus posed between the need for Governmental secrecy in some vital areas weighed against the public's "right to know." This dilemma has been accentuated because of America's leadership position in world affairs and its growing role during the last 20 years, and the budgetary demands that have been imposed that require all citizens to make human and economic sacrifices to sustain our national defense establishment.

Superimposed on this is the increasing difficulty which Congress has encountered in obtaining vital information from the Executive, particularly in the defense and foreign policy fields. If the public has a "right to know," Congress has a constitutional need to know as the people's representatives, so that it can act intelligently and responsibly as a coordinate branch of our Government—to investigate, legislate, and appropriate public funds for weapons systems, defense installations, and foreign policy programs as well as all of our other domestic activities.

I think that more or less summarizes what perhaps we all realize, but don't really think of very often in the larger context.

Going back to the history of Congressional interest, we recall that when President Truman issued Executive Order 10290 back in 1951 there was quite an outcry in Congress about some of the language in that Executive Order. In fact there were bills introduced by some of the more conservative Republican members of the Senate which would have, in effect, repealed E.O. 10290. So that today when we hear criticism of E.O. 11652 from the Hill, it's not a new exercise. This has happened in virtually every administration since the Truman years.

Some of the criticism has been constructive, we feel, in pointing out some problem areas that perhaps we'll discuss later and I presume you have already been discussing the last two days.

Other criticism is perhaps somewhat more political. But when you're dealing with an institution such as the Congress, and particularly in recent months where the confrontation with the Executive is getting a lot more hot and heavy, this is what you expect.

The Government Information Subcommittee, the predecessor of the Committee that I now work for, began hearings on measures dealing with the classification system back in 1956. Over the next six years there were very intensive series of hearings that probed every aspect of the classification system. These hearings concentrated mostly on the parts of defense activities but also included State and later the Space Agency and AID and many other agencies of Government that are involved in the foreign policy and defense areas.

I think it's noteworthy to look back and see just what triggered this kind of interest.

Many of you, I'm sure, will recall the Coolidge Committee that was established late in 1955 or early 1956 by the Secretary of Defense to look into leaks of classified information to the nation's press dealing with service responsibilities and their missions in the atomic age, which was then quite a controversial thing.

Shortly thereafter the Wright Commission was established by Congress—the Commission on Internal Security—so that there were actually three separate studies going on at the same time—the Subcommittee hearings, the Wright Commission's work, and the Coolidge Committee activity.

I think it's important to look at some of the recommendations that came out of the hearings that were held in 1956 and 1957 by the Government Information Subcommittee, which was then headed by Congressman John E. Moss of California.

One of the most significant results of these hearings was a report which was issued in the 85th Congress, House Report No. 1884 in 1958. And I'd like to read just a paragraph from that report. When I came across this last year, referring to all the work that had been done previously, I was amazed by the currency of the statement. It was almost as though it could have been written today. Perhaps you won't agree, but this paragraph from the 1958 report reads as follows:

> "Never before in our democratic form of Government has the need for candor been so great. The nation can no longer afford the danger of withholding information merely because the facts fail to fit a predetermined policy. Withholding for any reason other than true military security inevitably results in the loss of public confidence or a greater tragedy. Unfortunately, in no other part of our Government has it been so easy to substitute secrecy for candor and to equate suppression with security."

I think that is quite relevant today. One of the tragedies of any Congressional staff director's career is when he sees a subcommittee whose members spend literally years of their time and effort in carefully investigating a certain area and working sometimes for many months in

the drafting of a report based on those investigations, working weeks and weeks to line up votes and to change language to accommodate the views of others—and when you get 40 members of the Government Operations Committee to agree unanimously on anything, that's quite a feat. But the tragedy is once that's done and the recommendations are transmitted to the appropriate administrative officers in the Executive Branch, when nothing happens from those recommendations, when they're ignored, when they're overlooked, and when the problem as a result continues to grow and becomes more and more serious, this is one of the real tragedies.

Now, in 1958 in that same report I just read from, and in 1962 a report that was issued by our Subcommittee reviewing the operation of Executive Order 10501 after nine years of operation, the recommendations in those two reports I think were very significant. They were unanimous in the Committee on both sides of the aisle, regardless of political party. I feel that if at least three or four of these recommendations had been implemented properly at the time—1959, 1960, 1961, in that period of the 60s—it wouldn't have been necessary for President Nixon in March of 1972 to scrap E.O. 10501 and issue a new Executive Order. We're not yet quite sure how it's going to work. Our Subcommittee will hold some hearings after a reasonable time, probably next spring, to give the new Order an opportunity to be fairly tested. Those hearings probably will be coincidental with a bill to create a statutory classification system, which will be introduced shortly in the House.

Summing up very quickly as to the current hearings: in 1971 and 1972 the Subcommittee held several weeks of hearings at intermittent points on matters related to the classification system. They began in June of 1971 when the Pentagon Papers controversy was very much in the news and continued last spring—a very intensive review of exemption (b)(1) of the Freedom of Information Act which deals with national defense and foreign policy, also the procedural operation of the classification system, and some discussion of the new Executive Order 11652 which had then just been issued and had not even taken effect.

The results of those hearings is a report which is House Report No. 93-221. It is entitled "Executive Classification of Information—Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act."

I brought some copies here with me for those of you who may not have seen it. If you want it—I'll just leave them on the table and you can help yourself. If they run out and you still want a copy, please call the Subcommittee office at 225-3741 and we'll be glad to mail one to you.

This report was adopted on May 22 of this year, not quite two months ago. It is a very comprehensive summary of the hearings the Subcommittee held. It goes into the historical background on the classification system, which may be of some interest to you. Much of the research for this historical section was done by Mr. Dallas Irvine who is a historical researcher at the National Archives. He may be here, I don't know; I've never met him, but he had done some very excellent research. His study traces the classification system back to its very earliest beginnings.

The report finally lists some of the major defects in Executive Order 11652 and provides some recommendations on how the classification system might be improved by enacting a statute—what ought to go into that statute from the standpoint of the basic criteria of any good classification system.

I won't repeat any of it. It's over 100 pages long. It's quite comprehensive and quite controversial, I realize, outside of the Congress. I should point out, however, that this was a unanimous report of the full Government Operations Committee which is now composed of 41 members, 23 Democrats and 18 Republicans. It's a very interesting Committee, covering the broad political spectrum. Getting a unanimous report out of that Committee is therefore quite meaningful.

I have about 15 minutes before I must go and I don't want to leave without having the benefit of some of the exchange of views which I know is possible from this audience. There's nobody that's closer to the day-to-day operational problems involved in the classification system than the people in this room. And if you would indulge me to take questions out of order, I would be very pleased to proceed.

Question (Mr. Garrett): Could you suggest briefly the reasons why the Committee feels that there is a need for a statutory basis for a classification system?

Mr. Phillips: Yes. All the study that the Subcommittee has done since 1956 has persuaded us that no Executive Order classification system, no matter how carefully it's written, can really work, because the administrative problems are just too great and the legal sanctions are not there to give it any muscle. Despite lip service to imposing discipline against over-classification, despite numerous recommendations over the years by our Committee, despite assurances by Secretary McNamara in the 60s—"when in doubt, under-classify"—this has just not happened. And we don't believe that any administrative system issued under an Executive Order which has no force of law whatsoever—only administrative sanctions against the people in Government and to contractors to the Government—(the only ones who are covered by it) we just don't think it will work.

Now maybe a statute wouldn't work well either at first but these are things we're going to explore. And I assure you that Congress is not going to enact any law until it's totally persuaded that that's the proper approach. This is what's intended to happen under our system of Government through the legislative process.

There will be very extensive legislative hearings on any such bill. I would hope that spokesmen from this society would testify at those hearings because you all have a very great stake in what happens, as we all do. But what I'm trying to do is reassure you that there will be no precipitous shoot-from-the-hip action by the Congress without fully exploring every aspect of a statutory approach. This report which recommends that approach is the first step, based on the investigative hearings that we have held in the House, and which Al Friendly will, I'm sure, address himself to on what's been done in the Senate side.

Question: One quick question is if this is enacted in the law then, will that just in essence nullify the Executive Order?

Mr. Phillips: That's correct. It would repeal it. New

regulations would have to be written in each department based on the law.

Question: If over the years Congress has recognized these problems, what has prevented them from enacting heretofore an appropriate statute?

Mr. Phillips: This is the first time that Congress has ever recommended the replacement of the Executive Order system by a statute. I think it's a gradual evolutionary process. I think many members of Congress would personally prefer the system to operate under an Executive Order if it would work.

I think that the study that the Rehnquist Committee did during 1972 on the operation of E.O. 10501, the study that our Committee has done on the operation of E.O. 10501, and the indictment that the President himself has made in his statement that accompanied the release of his new Executive Order was one of the most damning statements that has every been heard as to why the Executive Order system won't work.

He spelled it out, chapter and verse, and in many ways he was repeating some of the arguments that the Subcommittee was making in 1958 and 1962, but it took 14 years to come to the point where there was a genuine desire to replace it.

Now, I hope I'm wrong, but from what I've been able to see, looking from the Hill to down town, the new Executive Order really hasn't changed things that much. I don't think it's going to eventually work any better than the old one.

Member: Well, it appears to me one of your strongest reasons for an Act is that the Executive Order may not have sufficient muscle. Certainly this must have occurred to Congress years ago in previous Executive orders.

Mr. Phillips: Yes, indeed. But these are things that under the Executive Order system the Congress can't change. The Congress can pass a law. The Congress can investigate how that law is working, but it's up to administrative implementation within the Executive Branch to really make it work. Congress can't do a thing about that on a day-to-day basis. Nor can any committee staff. It's really something that under our system has to be delegated right down to the agency and department level.

Now, if a law were enacted there would be certain criteria that would be spelled out so that it would apply across the board. There would be ground rules that would not just apply to the individuals who use classification stamps but apply to everyone, and everyone would know what that law was, what their obligations were under it, and what administrative sanctions, what administrative procedures, would be adopted to implement that law. It would be more subject to Congressional oversight than under the present system where the National Security Council, in effect, the Interagency Classification Review Committee, is a creature of the White House; and we have many problems as far as the White House is concerned in these days at least in obtaining access to information. We have gotten very little cooperation out of the Classification Review Committee. We have to beat them over the head even to get a document.

So we in Congress look at this issue as a two-way street. We want to be constructive and cooperative in this area, but we expect some cooperation from the other end. And we just aren't getting it.

Question (Mr. Robinson): One of the things suggested yesterday is that the Executive Order applies really only to the Executive. Under the law of course it would apply to all branches of Government, I believe; is that not true?

Mr. Phillips: That's correct.

Question (Mr. Robinson): Is there any comment on the views concerning Congress itself, which has been in kind of an awkward position, it seems to me?

Mr. Phillips: Well, I think this has been in a state of flux, but many of the events in recent months are crystallizing this issue. The hearings of Nedzi Committee has been holding on CIA and use of CIA property and personnel for illegal activity, and the Watergate hearings are undoubtedly going to have an effect on the whole climate of relationships between the two branches of Government and, in fact, have already had an impact.

The trouble is, with Congress it's not so easy to separate out this issue and say we'll consider it without any emotional or political overlap from other issues. It just doesn't happen that way.

There are many members of Congress who feel very strongly that this is the time for Congress to move in and to reassert some of the prerogatives and powers which it delegated to the Executive over the last 30 years. And this is one of those areas.

I think it's also significant to note a statement in the (Mink) decision by Justice White, who concurred in the majority decision but said that it was very clear to him—I'm paraphrasing—it was very clear to him that Congress could at any time assert itself and enact a statutory classification system to replace the Executive Order. In other words, if Congress was not happy with the Mink decision and the interpretation placed on the exemptions of the Freedom of Information Act in that case, it could always enact a statutory system. In effect, that's what our report recommends.

Question: I'd be interested in what sort of criteria you could recommend that would include the current system of classification.

Mr. Phillips: Basically, there are eight criteria that have been discussed. All of these are not spelled out this clearly in the report itself, but I think we would all agree on some of these. Some are so basic that you would hardly even think to mention them. For example, to provide for precise definitions of truly vital categories of information that are subject to classification.

Now, in one respect, I guess E.O. 11652 did go a little further in defining Top Secret, Secret, and Confidential because it did use a couple of examples of the types of information that would be included in each of those three categories.

Secondly, classification authority should be strictly limited to relatively few Executive departments and agencies directly involved in national defense and foreign policy matters, intelligence gathering and similar related functions. Here again this is one step that E.O. 11652 did take. There has been an historic reduction in the number of agencies and departments with orginal classification authority since the early 50s with E.O. 10290.

Third, only key policy-making officials of those departments and agencies should be trusted with original classification authority. They should be clearly identified in each document they classify, shall be held fully accountable

for their classification judgment, subject to severe and enforceable disciplinary action for abuse or misuse of their authority.

On paper E.O. 11652 goes in this direction. We are not persuaded that in practice it is being carried out.

Fourth, to provide for relatively short time periods for the vast amounts of more routine classified information to remain frozen in each category, and establish a workable administrative mechanism for regular periodic review, downgrading, and ultimate declassification, based on the determination of the need for the continued protection at the various classification levels.

Such determinations are not always measurable in absolute time periods as they are dependent on rapidly moving sequences of events involving scientific development, defense technology, changing diplomatic and military situations, and the like.

I think this is a very important factor that has never been taken into consideration. All of our classification systems have had fixed time periods, whether it's 12 years with a 3-year downgrading or 10 years with a 2–8–6; whatever the system, it has always been a rigid time frame. We think there ought to be a lot more attention paid to the continuing need to maintain a classification marking because of the changes that are going on in the world and in our own country.

It may have occurred—particularly those of you in the scientific area—and I'm sure Dr. Callen will address himself to this—that scientific development can be so rapid, such as in the space era, in the nuclear field, and in weaponry, that perhaps there's no need to keep something classified for as long as 8 years, or 6 years, or maybe even 1 year in some cases. Why shouldn't a declassification decision be made on the factual situation that is involved, rather than on some arbitrary time limit?

Question: I would suggest that that's not the problem. The problem is once you get the classification on it, how do you get it off? You're talking about millions of documents. You're talking about millions and millions of documents that have a wide distribution.

Mr. Phillips: That's correct.

Question: Does Congress have the money for people to take a classification off?

Mr. Phillips: Well, I don't think it's a matter of money. I think it's a matter of desire. I think if Congress felt that was really going to happen, there would be no trouble getting the money. Congress doesn't have much confidence in the people who are making these decisions. That's the problem.

Besides, I disagree that when you declassify something you have to physically hold it in your hand and examine it. I think there could be millions of documents declassified merely by looking at the type of information, not the document itself but the time frame of the documents, when they were originally classified, and make a declassification decision with a stroke of the pen. For example, I think the documents relating to the Bay of Pigs could all be released, merely by signing a directive. The only thing that would have to be eliminated would be names of people involved who may still be living in Cuba, or informants of one kind or another, and specific references to intelligence techniques used. These things don't have to be eliminated physically from the document. All that would have to be done is a directive signed that before they are released this should be done. Then if a person from the *New York Times* comes in and says, "let me see the documents in 1960 that deal with the Bay of Pigs," somebody would look at that document before they hand it over and remove the name of the person who may be an informant or similar sensitive data that might be shown in such documents.

These are administrative problems but I don't think they are so overwhelming as many people think they are. They don't have to be.

Question: Is Congress primarily concerned with political type information, technical type information, or all information?

Mr. Phillips: It depends on the committee and it depends on the Members. It's hard to answer that.

Question: I'm not convinced that the public really wants to know detailed information on weapons systems.

Mr. Phillips: I don't think so either.

Question: If this is the great bulk of the information—

Mr. Phillips: But it's a chicken-egg situation—if someone has a legitimate right to ask for it he ought to be able to get it, unless it would fall within the exemption criteria, where there's danger of our national defense or would aid a foreign government or something like that—utilizing the Espionage Act provision or the criteria under the Executive Order.

In order words, whether people want it or not is not the measuring rod. It's whether it should be made available if someone does request it.

Question: Isn't that procedure available now through the present Executive Order?

Mr. Phillips: You refer to documents over 30 years or the over 10-year mandatory review provision?

Question: Or even through the Freedom of Information Act through a court procedure.

Mr. Phillips: Right, it is.

Question: So really there isn't a problem there if someone wants information.

Mr. Phillips: Well, the courts have been very reluctant to look behind classification markings. And I'm sure most of you are familiar with the *Mink* case.

The reason I have to leave in a couple minutes is because we are marking up amendments to the Freedom of Information Bill which would overturn the Mink decision and amend exemption (b)(1) of the Freedom of Information Act which deals with national defense and foreign policy information. What is proposed in our bill is to require the Court to review the classification markings on a document in an *in camera* procedure—which the Court refused to do in the Mink case—and which we think is absolutely necessary if the Freedom of Information law is to be effective.

Question: You mentioned nuclear weaponry. How is this proposed legislation related to the Atomic Energy Act, or would it be?

Mr. Phillips: I guess it would depend on what aspect of it.

Question: Would it deal with nuclear weaponry or has it been discussed?

Participant: The Restricted Data bit is what he's talking about.

Mr. Phillips: We have looked very closely at the AEC

system. In many ways it is a model in terms of periodic review and declassification procedures. They probably declassify a greater percentage of documents originally classified in the AEC's own system—the statutory system which is in the Atomic Energy Act.

I think these are questions that I just couldn't answer at this point. It depends on the precise nature of the information, how it's to be used, what its potential uses are, what it's related to, and all these other factors that are involved.

Dr. Callen: Mr. Phillips and Mr. Friendly are experts on the viewpoint of the Congress on this problem, and all of you are truly working experts who understand the details. I'm not. I'm saying all this because I was really terrified by all those probing questions that you asked Mr. Phillips.

I worked for some 15 years at the National Security Agency and the Naval Ordnance Laboratory as a working scientist and my experience has been just that of a Government worker in research who has seen something of classification because I worked in agencies which did a lot of classified work.

There are a couple points I'd like to make, however, that I think may be relevant. The first one is a scientific one and the second one is a political one.

The scientific one is this: that as a scientist I would see that when you work on a technical problem, something which is related to classified matters and national security, it's very easy to see the reasons for classifying it. This is something you don't want to have a foreign power get hold of. So the natural thing is to say, "We'll classify it so it doesn't get out and that way we'll protect the national security of the United States." That seems a useful thing to do, and I was very sympathetic to that.

But now I look back, and I realize that empirically it's very hard to make a case for that. Strange as it sounds it's very hard to make a case justifying that. Because there are other forces at play. That is, we live in an open society and the best way to make scientific progress and technical progress is by knowing what everybody is doing. Get the competitive system working, get lots of people interested in the question—in industrial laboratories, in Government laboratories, at the universities—so that they are working on it as a scholarly research activity or as an industrially productive field, and that way you make progress. Whenever you classify things you make it difficult for that exchange, that competition and exchange to take place. It's hard to see that, point by point, when some technical matter comes up. It's hard to see that by classifying something, what you're doing is reducing the ability of that interchange in the very community where you need this in order to develop technical competence.

Let's be a little objective about it and empirical. If you look at it empirically, you find in fact those areas which have not been classified, which have been open, are the ones in which we are preeminent, in which we lead the Socialist States, Soviet Union, whatever; and those in which we have been most cautious in classifying things are the ones in which we lag.

For example, NASA. NASA has essentially nothing that has been classified. I was on the Scientific Advisory Committee for several years. NASA did very little that was connected with classified work. There was some overlap between NASA and the missile program the classified missile program; they used missiles from the Army and so on. But basically almost everything NASA has done has been open, available to the community, widely known. The fact is that we started from behind in the space program after Sputnik. In a very short time we caught up and surpassed the Soviet Union. In fact, you know, last year we had a meeting with the Soviet Union to share information. The real purpose of the meeting was because the Soviet Union has been unable to do this docking feat that we're experts at and they wanted to find out how we do it. So we had a meeting at which that was on the agenda—for us to tell them how we dock. Of course we tried to get something in exchange for that.

One fact isn't enough. It was the whole mass of technical know-how that NASA developed. Leaking the facts doesn't help the Soviet Union. They didn't want to know how many threads there are on one screw or how you do this detail. It was putting the whole thing together with hundreds of thousands of details—how you measure, how you do this, how you hold that together—and that was developed by a free economy—competition, many companies exchanging information, open exchange—which developed a whole huge technical interlocking mass of expertise, which wasn't a matter of secrecy, it was a matter of being able to carry it out and do it. And we did it, successfully. We surpassed them openly, because we're an open society. So there we see by being open, we actually developed the technical expertise.

Now I'm convinced that if we had said this is a prestige thing. It's like military, we have to get ahead of them. It's a strategic thing, classify it—that we wouldn't have got there. Because then we wouldn't have known. One company wouldn't have told another. The Government wouldn't have been able to release the tests, and it wouldn't have developed as it did, I personally believe.

Another example is the computer field. The computer has always been an industrial thing. There has been no classification, virtually. True, there were many computers at the Agency where I worked. The National Security Agency sponsored a lot of the computer development and the money helped. Most of the work they funded to industry, but it was not classified work. Almost everything that has been done with computers has been unclassified.

We lead the whole world in computers. We lead the Soviet Union, we lead everybody in the world in computer technology. We did it through the open marketplace, by competition, by exchange of information, and by public knowledge. And that has protected us more than any secrets have protected us—that knowledge.

Another example is the semiconductor business. We've always dominated the world. We can compete with anybody in the semiconductor business. The only place where we don't compete is in Japan and that's because they don't allow us in to the Japanese market. If we were allowed to compete in Japan freely we would do all right in spite of the difference in labor costs, because we have the technical expertise. We're ahead in scientific and technical management—management, more than anything else, of how to carry a new technology through to completion and get it into the marketplace.

That's not a matter of secrets. It's a matter of techni-

cal competence. You get the technical competence, you will note, with open exchange of information.

Let me give you a counter-example: nuclear weapons. In nuclear weapons I'm no expert, but those who are—Edward Teller, who, I think you'll all admit is knowledgeable; he is father of the H-bomb—says that the Soviet Union knows not only every secret we have now but every secret we're going to discover in the next two years; because they're so far ahead of us.

Nuclear weapons is the preeminent field where we've kept everything secret, classified, and it hasn't protected us at all. What it really does is retard progress. So Teller is very much in favor of total disclosure in that field, nuclear weapons. If we disclose everything we know in nuclear weapons, we won't be telling the Russians a thing because they already know everything we know. But at least we'd be telling ourselves what we know, so we could talk to each other openly and freely and start to make progress for a change. This is what he feels has held us so far behind the Russians in this.

Let me read a couple of statements so you don't need to take my word for these arguments, but the word of more qualified people.

Here's an article called "Integrated Circuits in the Electronic Industry." It was written by someone named C. Lester Hogan. Les Hogan was a Professor of Physics at Harvard and then he went into private industry. He's now president and chief executive officer of Fairchild Camera and Instrument Corporation. I'm just going to read a few statements here and there from his article.

Here's one: "American technology has and can prosper in an atmosphere of international openness because competition always has brought out the best in us. The open society is our natural environment. Our country has done a superbly better job of managing emerging technologies than most countries of the world. One of the outstanding examples of technological management is, again, the Bell Telephone system. Bell has led in the development and use of an incredibly complex infinity of technical development. It has planned, organized, built, and managed the most extensive and complex electronic system in the world and has afforded to this country the best information handling and communications systems that exist and has done so while paying the highest salaries to its employees."

As another example, Hogan discusses NASA. He writes that the moon landing was a huge challenge—an untracked road for man to travel. Yet it was accomplished. And no secrecy was involved. Out of the space effort have come contributions to society which Hogan believes will be felt for many generations.

He says, "I use Bell and NASA as examples to show how technical openness properly managed not only can prove beneficial to others in industry but to the world as well. I believe we have nothing to fear by being more open on the technical front because America has one other characteristic which if continued will assure supremacy and rapidly expanding technology"—he goes on to talk about the competition system and the incentive reward system—"I believe openness is as important to the technical community as a politically open society is in providing the only truly successful route for mankind."

Here's another statement. This is by Dr. Teller. I'll read just a little of this on the freedom of scientific exchange.

"The attitude of scientists dates back to the close of the 18th century when the traditional secrecy of alchemy was broken. Since that time freedom of exchange was established and publication of scientific results became a duty.

"A reactionary trend did set in after the end of the Second World War. The worldwide shock caused by the use of nuclear explosives reestablished a measure of secrecy within science which as yet we have not succeeded in overcoming.

"There are many who believe that secrecy is needed for reasons of national security. The fact is that secrecy did not prevent loss of our leadership by the United States in the field of nuclear weapons. On the other hand, a much more open policy permitted the rapid development of electronic computers, in which field the United States has a position of undisputed leadership.

"Secrecy has erected barriers between our country and our allies. These barriers are harmful to science and are a source of weakness in the free world.

"Toward the end of 1945 Niels Bohr said: 'One should expect that in the cold war each side will use the weapons it can handle best. Secrecy is the appropriate weapon for a dictatorship, whereas openness is the weapon that democracy should use.' By sticking to our principle of openness and free speech we may bring about in the course of time a change of heart in Russia. Among our Russian colleagues we shall have many allies. While such a change will certainly not occur immediately, the long-term effect may well be more salutary than any formal agreement that one can imagine."

So that's one of the points that I wish to make: that this natural desire to classify something because it's something which we wouldn't want others to get hold of has another side. This is the other side. You're also classifying it so that we ourselves can't get hold of it. And in fact the empirical evidence is, if you look at the cases, that classification has been our own worst enemy in scientific and technical matters.

The other point I want to make—this is a hard one to swallow, because I know that all of you look at yourselves as technical experts doing a professional, non-political technical thing. You understand the Executive Order and you implement it.

The fact is that whether you like it or not, what you do is unavoidably a political thing. That's an unpleasant fact to recognize but it's simply true—not because you do something political, but because the fact is that classification has always been used politically. Not so much in what is classified, but what the Executive Branch chooses massively to release. They do it all the time. You don't do that, of course, but the fact is that the classification system can't be divorced from the political implications. It has been said that the ship of state is the only ship that leaks from the top. That is the way the Executive Branch uses the classification system, as a way of keeping the Congress and keeping the public from knowing things. Every newsman knows that one principal source of his information is leaks, massive leaks to friendly newsmen of classified material. So you have to recognize that. It's not purely a technical thing—that you are part of a system

that has political implications all the time.

Just look every day in the newspaper and you see that. I cut out from yesterday's paper this business about the Cambodian bombing. Let me read a little of it to you: "U.S. bombing strikes that were launched against neutralist Cambodia in 1969 and 1970 and were subsequently disguised as attacks in South Vietnam numbered in the 'hundreds' each month for 14 months," the Pentagon said yesterday. Assistant Defense Secretary (Jerry W. Friedheim) said the "same special security precautions that were used in the Cambodian raids were employed in Laos to keep the attacks secret." Friedheim also said that details of the bombing in Cambodia and Laos were given to only a few members of the Senate Armed Services Committee. In what he characterized as "normal" procedures of Pentagon accountability to Congress. Friedheim said the bombing information was withheld from other members of the Senate Committee, including those who opposed U.S. war policies at the time. According to Congressional sources, the members of the Armed Services Committee who were notified were the chairman, Senator John C. Stennis and Senators Barry Goldwater and Stuart Symington, all of whom supported the Nixon Administration's Vietnam policy. Senator Harold E. Hughes, who was frequently critical of the war policies said he was never notified of the raids or the military decision to file falsified post-strike reports which erroneously showed that the bombs had been dropped in South Vietnam. In fact Hughes complained that just a month ago the Pentagon sent him a detailed listing of Southeast Asia bombing operations that failed to mention any strikes in Cambodia prior to April 30, 1970. The report goes on to describe the way the Pentagon falsified documents. Friedheim admitted that they purposely did not give the information to members of the Senate Armed Services Committee who were opponents of Pentagon policy.

That's one example.

This is another example of the same sort of thing. This is about the SST. It has to do with Executive privilege.

During the SST debate, President Nixon put together an illustrious panel of experts to give him recommendations on the SST, among them the President's Scientific Advisor and Richard Garwin of IBM.

The panel wrote a report which said that regarding the effect of the SST on the upper atmosphere "a fleet of SSTs will introduce large quantities of water vapor into the stratosphere," and they didn't know what the effect of that water vapor would be, that it might be dangerous and it shouldn't be put into the atmosphere until we know what large quantities of water vapor would do to the atmosphere.

With regard to the impact of the SST sonic boom, the panel said, ". . . all available information indicates that the effects of the sonic boom are such as to be considered intolerable by a very high percentage of people affected." Finally, as to the impact of the SST engine noise, the panel said, ". . . over large areas surrounding SST airports, . . . a very high percentage of the exposed population would find the noise intolerable and the apparent cause of a wide variety of adverse effects."

With this report before him, the President recommended construction of the SST. William McGruder, his represenative, director of the SST project testified before Congress. With the report in his possession, he testified, "According to existing data and available evidence there is no evidence of likelihood that SST operations will cause significant adverse effects on our atmosphere or our environment. That is the considered opinion of the scientific authorities who have counseled the Government on these matters over the past five years."

Now, Garwin, who was on the committee, knew that wasn't what the committee had said. He told Representative Henry Reuss about that. Representative Reuss asked the Administration to release the report to Congress, and the President invoked Executive privilege and said, "No, you can't see the report."

Well, you see, the report didn't say at all what William McGruder said it said.

Now of course that's Executive privilege; it's not classification. But there are a thousand examples of that. Max Frankel in his affidavit for the Pentagon Papers gives dozens of examples of selectively classified information given to the press. So it's something you just have to recognize, that you simply can't divorce what you do from the political process. Not what you do—of course you do what your job is. Your job is to implement the Executive Order and you do that, of course, to the best of your ability and as honorably as you're able. But the fact is that the process itself has political implications and it's massively subverted for political reasons. I think it's something we just have to live with. It's a fact of life.

There's one more point that I would like to make before I stop. That's again about this matter of what kind of national security information should not be covered by the Executive Order. This is the exemption category we were talking about.

Because of this kind of thing that happened in Cambodia and Laos, I hope that we have learned that there is a certain area of military and national activity that we should simply say, "No, that cannot be classified."

The Executive Branch shouldn't be able to go on military operations, carrying on a war, without letting the Congress and the American people know about it. Why do we classify war in Cambodia? Surely the Cambodians knew they were being bombed. The purpose of such classification is to keep the American people and the Congress from knowing. And surely the President and the United States should not be able to wage war and keep that fact a secret from the American people. So this is a particular area of national military activity which should certainly never be classifiable.

The need and the right of the people to know outweighs any Governmental interest in concealing military action the Government is taking or sponsoring. The presence of U.S. military or paramilitary forces in foreign countries, the provision of U.S. military or economic assistance to foreign countries, and any diplomatic commitments the United States has made to do these things should be made known. I think these things should be explicitly excluded from the Executive Order.

Mr. Friendly: I want very much to pick up something that Dr. Callen said before. I know you've talked about S-1400 and specifically Section 1124 which is the section which provides criminal penalties for the person who, having authorized possession of classified information, discloses it improperly. The panel, as I understand it, is on

Congress' view of the Executive Order.

One of the arguments that the Administration has made for Section 1124—and they admit that the section goes beyond recodifying present law to introduce a new element into the law—is that the Executive Order provides a review facility, review channels inside the Administration for people who do have authorized possession of classified information to challenge the classification. That's dandy, except no one is using those channels, and no one is likely to.

We have had hearings in the Senate Subcommittee on Intergovernmental Relations and with a couple of other subcommittees on this problem generally. We haven't done anything like the detailed work they have done on the House side. But in one of the hearings Senator Muskie asked Bill Bundy what would happen to somebody in the State Department, for instance, who looked at a document on his desk and said, that belongs in Confidential—it's classified Secret or Top Secret—and started a procedure within the review channels of the State Department to get it declassified or at least to contest the classification. And Bundy just said, "He would be regarded as rather poor promotional material."

The argument speaks for itself. The only empirical data we have are from Dr. Rhoads, who has been cooperating with our committee. I'm frankly hopeful of continued improvement in relations between the ICRC and the Congress—there are a number of political means that I don't think are necessary to explore. However, Dr. Rhoads came up and testified and he made the point that there have been since the new Order came into effect in June 1972 to the end of March of this year some 350 mandatory declassification review requests; of which only one originated inside the Government and that happened to be from a fellow in the Archives who actually wanted Clark Clifford's papers from 1949 and 1950 declassified. They are in the Truman Library and I believe they were declassified. So out of 350 there was only one from the Government.

I, personally, and I don't think I can speak for the Congress—I, personally, am not satisfied that the review procedure in the Executive Order is going to be implemented without added incentives. Until that review procedure works I do not think the Congress will accept the proposition that you can impose criminal penalties on an action for which there are only administrative remedies. So I would say that 1124, given the existing Executive Order, stands a very, very poor chance of enactment; or any kind of legislation which simply takes the fact of classification by itself as the determining factor of criminal action. This is not going to wash in this session of Congress.

I gather you talked about the Ellsberg case, and someone made the point that if Ellsberg had been acquitted, the atmosphere in Congress would be different and there would be a great deal more pressure retroactively to get Ellsberg. As it happened, that case ended in disorder and confusion, and that's the status of the law now.

To confuse matters further and to pick up a little of what Dr. Callen was talking about on the political nature of classification, and what Bill was saying about putting a statutory basis under classification, I'd like to talk about the thrust which I see developing on the Senate side—which is to say we've got a classification system. It's a house-keeping system. It's an administrative problem in the Executive Branch and it's terribly difficult to implement, terribly difficult to control, and it's terribly, terribly difficult, as someone pointed out, to write criteria that someone walking in fresh can understand and can automatically determine from reading a document or looking at a record in front of him how to apply the classification system.

So the thrust that I see is for the Congress to try and inject itself into the system, not necessarily by writing a statutory basis for the system but by providing a review of its working, an ongoing, binding review. There's a little bit of evidence to support my conjecture, aside from the fact it happens to be my personal interest in approaching the system. I don't think the Congress is capable of administering the classification system. I don't think it's even capable of writing criteria that are a lot better than the Executive Order at the moment or what are developed in implementing the Executive Order in the agencies.

What I do think the Congress is good at and what I do think the political pressure is moving toward is the usual job Congress does—which is oversight. We see one portion of a bill Congressman Moorhead introduced last year which was based on a bill that Senator Muskie had put in December of 1971 that would have set up an independent classification review commission—I don't know that that's what it was called. Senator Muskie called it a disclosure commission and Congressman Moorhead called it something else. The Republicans have presented it now as the Freedom of Information Commission which would have some jurisdication over (b)(1) situations. Everybody's got a different way to compose that commission. The latest proposal has the judiciary appointing everybody on the review board. The Moorhead bill I think was a 3-3-3 proposition, 3 from the Executive, 3 from the House, 3 from the Senate. In Senator Muskie's bill, one man on it was to have journalistic background, one with a diplomatic background, one lawyer, and so forth—a nice picked bag of people who would do two jobs, which is one of the problems. They would judge challenges to classifications and also they would crack the whip over the whole spectrum of classification management. I don't think the two jobs are compatible myself.

The other thrust is simply to have a Congressional body itself that keeps an eye on things and raises hell when they go wrong, that embarrasses you or your bosses quite frankly, probably your bosses.

You will find that idea in two resolutions that are in the House to set up a new joint committee. You will find it in my desk drawer in a bill that may never get introduced. It's not in the Gravel bill. The Gravel bill has the commission idea still. The idea is floating around. Representative Mink has a proposal she hasn't introduced. The concept probably would be a joint Congressional committee based on the argument that the only people who can supervise, who have the right to challenge the decisions of adminstrators, are elected officials, not other appointed officials but elected officials. This joint Congressional committee would in one fashion or another lay hands on the whole operation of the classification system and grab at those little bits and pieces of it it could find

that weren't working right.

Now any law that set up that committee would also have to go into criteria and have to say on what basis the joint committee would challenge a classification or a classification practice. But my own feeling is its major role would be that of raising hell, probably pushing some things into the courts where there were disagreements.

Mrs. Mink's bill would give the committee statutory authority to declassify anything a member of Congress brought to it and said shouldn't be classified. I think the first time they did that, you'd have a fascinating court case. I think you'd have a court case anyway if the commission simply ordered—as in the bill which is in my desk drawer—simply ordered the declassification date changed on a document when it came before it for review.

But the real question in my mind is whether there is any way to review the system at all, and I think, thanks to the Executive Order, there may be the beginnings of a way. You can't review something that you can't know, that you can't conceive. There is some evidence, although not at all conclusive, that there may at last be a way to index what is being classified. I'm not going to talk to all the historical material and all the problems in that field. I'm just going to talk about ongoing classification.

If that material is being indexed inside the agencies, if the agencies are submitting reports on their indexing operations as they are supposed to under the Executive Order to the ICRC, then they could submit the same reports to this joint Congressional committee and perhaps do a more detailed report on a fairly regular basis.

There would be one hooker in this too. The law would say that nothing that isn't in the index can qualify under (b)(1) as exempt from disclosure, so you would make the index itself a measure of what the Administration regards as meriting protection under the law.

There are various ramifications of that too into the criminal law, but let's just stick with the idea that you could develop a central index.

The ICRC's function, it seems to me, could be a first review. Maybe it would be the final review. Maybe we'll never get the joint committee. Maybe we'll just have to beef up the ICRC. I'm not impressed by the fact that the one permanent staff member it had has now gone back into law practice in New York. I don't think that's a very encouraging sign as to the efficacy or spirit with which the ICRC is capable of approaching an enormously difficult job.

So let's say that the separate indexes were first submitted to them, and went from the ICRC up to a watchdog body in the Congress. What should be on the index?

This is going to be your problem. I assume some of you have even been working on indexes and even on moving from manual to computerized information. The important thing for Congress obviously is to be able to see from the index what is being classified. The way it can raise hell is to find out that the USIA is classifying on a monthly basis a vast volume of documents that it has no business classifying. Simply the number of documents will give you a clue to the fact that somebody at the USIA has gone batty over secrecy. A member of the USIA can be called up to explain why they're doing what they're doing.

But the index at least in terms of the requirements that the ICRC put out last December and revised in January, would have two elements which I would think would enable the Congress to look and see—honestly it's going to be the staff of that joint committee—the title or description of the document, and the subject matter in those terms; in other words, some guide that goes a little beyond the title, that tells you what's in the record that's being preserved and why it's being preserved.

The real hope of course, is if you have that, plus the declassification date, the agency where it was classified, the exemption from the declassification schedule if it is so exempted—that a computer printout will give somebody in the Congress a way to grab handholds on the system and basically to oversee, to review. Because in classification, if it is, as Dr. Callen believes and I believe, a political system not in its implementation but in its effect, the important thing is that there be someone beside the original classifier who decides whether or not that decision to classify and maintain classification for a certain period of time is justified, and politically justified. If there are no other criteria, it is a political decision, political in terms of your decision about science and the merits of sharing scientific knowledge with the whole scientific community. Somebody on that joint committee is going to have to be able to go to Dr. Teller or a group of scientists and say, Does this formula really have to be—does this paper really have to be kept Secret for six months? What's going to happen if it is?

I think the Congressional committee will be in a position to ask for outside advice on a scientific matter and raise hell if there's a justification for it.

But the question in all this is: Can it be done; can an index that anybody can read and work from actually be put together? The Justice Department says yes, and I am told they are indexing absolutely everything that's classified. The CIA, I gather, is classifying only what it calls finished intelligence and not working papers.

Well, when we write the law—if we write the law—we're going to have to say how far up the line this classified paper has to go to get on the index. Should something that stays on a man's desk for two weeks while he's writing a report and then goes into the burn bag be indexed? Maybe yes, maybe no. It's a very difficult decision. And I'm sure the CIA's solution is the reasonable one.

NASA, I gather, is just indexing its finished reports as well. The Atomic Energy Commission under the long-standing provisions it has is already, I'm told, computerized, automated, and complete.

The rest of the Government—I gather the State Department is trying, the Defense Department is not trying—I suppose I shouldn't say that. Based on my information, they are thinking about trying. USIA, I'm told—and there may be somebody here that will correct me—is still a manual operation. It's not heavy volume. AID is trying. The Transportation Department hasn't made much progress under the December 1972 instructions from the ICRC. GSA and Treasury aren't significant problems.

But the problem for Congress is to try and write a law, if this index is a workable tool—first of all we're going to have to hold hearings to find that out—with a view to putting the indexes together, whether or not it can be

done, how much it's going to cost—to go back to your question. The Congress is going to have to recognize the cost and agree that the cost is important and agree to authorize whatever it takes to do it.

But then the question is what can be on that index that will give a clue to the Congressional committee as to what is being classified and what is being classified improperly. That's the only thing they're interested in. They are not interested in what is being classified properly. They're not going to be interested in the bulk, the vast physical bulk of defense contracts. Very few of those, I would suspect, will ever be challenged in any detail. The problem is a political one. The problem is also a scientific one. The thrust of review, whether it's done by that Congressional committee or whether it's done by an independent commission, is going to be to embarrass you. I don't think there's any way around it. It's no aspersion on your character or your competence. It's the balancing act in the Constitution between security and the First Amendment. The Congress, particularly this Congress or the Congress in the Watergate Era, is going to be pushing hard on the First Amendment. In the next Congress that joint committee might just wither away. The problem might wither away.

I have a very strong feeling that the Executive Order, if it's carried out energetically by the Executive, is the solution. But if you can't get the Executive to do it and if you can't keep a guy like David Young in there to do it without getting into other kinds of trouble, then the Legislative Branch is going to come in. We have deferred for a long, long time to the Executive. In the aftermath of the Watergate, and as Bill said, I think we are going to write some kind of a law.

You can see that there is considerable difference of opinion between Bill and me as to what kind of a law we're going to write.

Questions and Discussion

Member: I wish to make a statement, you might say on classification versus freedom of speech and so forth of information.

A fact not well known to many people is the fact that the Army was all ready two years before they launched the first satellite; we could have beat Russia by a year. But here again, the political atmosphere, not the classification, was the hindrance—interservice rivalry and so forth, the Air Force, the Navy. There's a little plaque down at Redstone Arsenal that says: Explorer slept here two years.

Now here again we were probably first, ahead of Russia, in the technological area, but the political atmosphere—

Dr. Callen: Was the political atmosphere in any way conditioned by the secrecy surrounding it?

Member: No. It was all open.

Dr. Callen: It was just we wouldn't spend the money?

Member: No, they were using different services. I think the Air Force had preference, and then they got the missile, you know.

Member (Mr. Bagley): They wanted to divorce it from the military applications and they assigned it to the Navy under the Vanguard project.

Member: But I want to go back. Many times the security classification, I agree, is a hindrance to freedom of flow of information but not always necessarily. There are many other areas of holdup—inertia in certain things that you just can't push through is more of a hindrance than the actual classification.

I agree there should be some type of watchdog system to challenge such classification, especially continued classification—

Mr. Friendly: I think Bill just didn't talk about it but I think in the Moorhead bill last year it sounds as if that is what he was talking about. There was the watchdog as well as—there were both things, the statutory basis to the system plus the watchdog. I've got real problems with the watchdog if you take it outside the Congress and the courts and set it up as an independent body.

Member (Mr. Bagley): I cannot resist at this point telling you that the Presidential Science Advisory Committee at that time recommended to the President that an intercontinental missile was not technically feasible. This was in 1954 and 1955. So when you are talking, of PSAC and its bodies and its infallibility I always remember that one.

Question (Mr. Garrett): Dr. Callen, would you recommend open publication of all scientific developments?

Dr. Callen: Well, of course, scientific developments insofar as they are scientific developments, almost entirely are openly published now.

Member (Mr. Garrett): Going beyond basic research.

Dr. Callen: That's hard to face, but I have to say yes. Looking at it empirically, except for very special areas, I think when you look at it in retrospect you realize we'd be better off to do it that way

Question (Mr. Garrett): If we did do that, would we just hand them out and make them available to everyone?

Dr. Callen: That's the point. In those areas where we have made it available to everyone, we dominate, not because the Russians don't know this fact or that fact but simply because we have such an enormous expertise in management and R&D and development that we can just carry the field, because of superior competence. That's what we did in the semiconductor business and that's what we do in computers, not because we keep secrets from them. We're just technically better than they are. We function better in an open society.

Question (Mr. Garrett): Would this then not eliminate much of our quid pro quo possibilities?

Dr. Callen: You don't need quid pro quo with computers. Almost everything accomplished is solid state physics and in computers and the semiconductor business comes from us first. There's very little we need to exchange with the Russians in those fields because we're simply so good at it.

Furthermore, anything one country can do, another country can do a year later if they put their mind to it. Basic research is published openly. It's a matter of application. Anything France wants to do, they can do within a year. If they decide they're going to make a bomb, they can make a bomb.

Question (Mr. Garrett): We have spent millions and millions of dollars on it and give it to them free?

Member: Right. Why shouldn't they foot the bill?

Dr. Callen: We give it to ourselves free in order to be ahead.

Question (Mr. Garrett): Where does the quid pro quo come in? We give them anything and we get nothing back.

Dr. Callen: Why do you want quid pro quo? What we really want is security. What we really want is technical expertise, leadership. Openness gives us security.

Member (Mr. Garrett): Quid pro quo may not be scientific. It may be political. It may be a number of things.

Dr. Callen: Your argument is that we should penalize ourselves and hold up progress so that we don't give them things which will allow them to make progress?

Member (Mr. Garrett): Isn't the reason for holding back nuclear technology so as not to provide break through to N^{th} countries? That's the main reason for it. We have enough countries in the world now with nuclear weapons. We don't want any more. If we published all of our papers on nuclear weaponry developments, any country in the world could pick it up immediately.

Dr. Callen: Almost any country in the world that wants to can do that now. The main thing with a bomb that holds some countries back is the delivery system. It's easy to make atomic bombs. The hard thing is the placement and that's a technological feat, you know, the ICBM.

Of course the thing is when you get right down to it suitcases do very nicely. A little country doesn't need a big ICBM, just a couple people meeting in a sewer with a suitcase.

Question: One question on the data index system that you mentioned. I feel that it's wonderful but it seems to me that it would be very cumbersome and very expensive.

Mr. Friendly: Isn't it necessary though?

Member: That's my point. I think it can be accomplished but not under the Executive Order.

Mr. Friendly: Even under the Executive Order if the push is on to get it.

Member: In selected categories.

Mr. Friendly: Right. This is the problem, selecting categories. That joint committee, if it ever came into being, has not enough time nor really the inclination to want to see computer printouts for 200,000 pieces of information monthly, yearly, whatever it is, so the problem is selecting categories. ■

SECRECY AGREEMENTS AND STATEMENTS INVOLVING CLASSIFIED INFORMATION

Mr. William G. Florence,
Security Consultant

Discussion of secrecy agreements is quite appropriate at this classification management seminar. The signing of a statement promising to protect classified information makes an individual vitally concerned with the true meaning of an assigned classification. The integrity and credibility of both parties to a secrecy requirement is laid on the line—the one responsible for imposing classifications as well as the one agreeing to observe them. As a further concern of this Society, now and on to the Seminar Theme Year 1980, the efficacy of classification and declassification practices determines whether a secrecy agreement is good or bad.

We have reviewed the purpose of security classifications, and discussed their application in practical situations. As provided in Executive Order 11652, the security classification system should apply only to official information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

Procedures for protecting an item of classified information are stated, in abundance, in the Executive Order and related regulations.

First, of course, is the initial determination for access:

> "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 is necessary for the performance of his duties."

A threat of prosecution is reflected in the following notation prescribed for use on documents, although the Executive Order cites no law as a basis:

> NATIONAL SECURITY INFORMATION—
> Unauthorized Disclosure Subject
> to Criminal Sanctions

Numerous other regulatory procedures are stated for physical protection of material containing items of classified information. They include: category marking, reproduction, storage, transmission, and destruction. In fact, the Executive Order and regulations tell the people to whom they apply everything they should know about safeguarding an item of information bearing a classification of Confidential, Secret, or Top Secret.

But, there is a peculiar problem about a security regulation. It cannot protect information. People, not regulations, keep secrets or broadcast them. An individual having knowledge of information classified either by himself or someone else will disclose or withhold it as he chooses.

In the light of this fact, some of the Executive Branch agencies require that their employees sign a secrecy agreement or secrecy statement. Also, many people outside the Executive Branch must sign a secrecy statement. Apparently, the primary purpose of the agencies is to demand that an individual promise not to reveal information bearing a classification marking, regardless of how innocuous it might be in relation to the national defense—or how helpful it might be to the American people.

I will review with you the Central Intelligence Agency (CIA) secrecy requirements, as applied to Federal employees. The validity of two CIA secrecy forms was subject to court test last year in a civil suit for legal analysis of alleged contractual violation.

I will talk also about the Department of Defense "Security Briefing and Termination Statement," DSA Form 482, as applied to contractor employees. That form probably has been signed by, and has affected more people than all other forms combined. It too went to court this year in a criminal case—the Ellsberg-Russo trial.

Before exploring specific provisions of secrecy forms and policies calling for their use, it would be appropriate to reflect upon certain relevant basic facts. They have existed all along, but have been largely ignored by many people intent on honoring assigned security classifications.

- The assignment and retention of a security classification is strictly a matter of mind. An administrative regulation can authorize a person to decide for himself, on his own reasoning, that information revealing a proposed or completed action warrants secrecy. The same regulation can permit him or his superior, on up to the President, to think differently immediately, and treat the information without secrecy according to his own need or wishes. Whatever classification marking might have been put on a document containing the information can remain intact and entrap another individual, perhaps at the cost of his security clearance or his career. (Reference: Executive Order 11652)
- The Federal copyright law provides that "no copyright shall subsist in . . . any publication of the U.S. Government . . ." Under such restriction, the Executive Branch can only strive to control knowledge of its own use of an item of information, such as the application of it in a weapon system for national defense, or in a Government patent. (Reference: 17 U.S.C. 8)
- Under the First Amendment of our Constitution, there is no basis for the Government to impose prior censorship in the name of national security on *private citizens generally.* (Reference: U.S. Supreme Court action permitting publication of the Pentagon Papers)
- The First Amendment *limits* the extent to which the United States, contractually or otherwise, may impose secrecy requirements on an individual as a Federal employee, and enforce them with a system of prior censorship. (Reference: *U.S. vs. Marchetti* Fourth Circuit Court of Appeals No. 72-1586 and 72-1589; also, U.S. Supreme Court No. 72-482)

At this point, I sincerely suggest that anyone who waves the American flag of loyalty over the alleged sanctity of administrative security classification more than the First Amendment could well reexamine his sense of relative value.

Let us review the two CIA secrecy forms. One is designated "Secrecy Agreement." A person must sign it upon being employed. The other is a "Secrecy Oath," which he signs upon separation.

The relevant extracts of the Secrecy Agreement are:

> I, (name), understand that by virtue of my duties in the Central Intelligence Agency, I may be or have been the recipient of information and intelligence which concerns the present and future security of the United States. This information and intelligence, together with the methods of collecting and handling it, are classified according to security standards set by the United States Government.
>
> I do solemnly swear that I will never divulge, publish or reveal either by word, conduct, or by any other means, any classified information, intelligence, or knowledge except in the performance of my official duties and in accordance with the laws of the United States, unless specifically authorized in writing, in each case, by the Director of Central Intelligence or his authorized representatives.

Those three sentences do the job. There is another sentence which refers to understanding the espionage laws concerning disclosure of information relating to the national defense. But there is no suggestion that disclosure of information would violate the law because of classification.

The CIA Secrecy Agreement was ruled to be a valid contract by the Federal District Court and the Fourth Circuit Court of Appeals last year in the Marchetti case. The essential element, a proper consideration, was deemed to be *employment.* The mutually agreed secrecy provision, as expressed in terms of CIA related classified information and intelligence, was deemed *not* to violate a person's constitutional rights. This seemed to be based on the commonly accepted view that the Government necessarily has a right to strive for secrecy regarding information directly related to the active defense of the nation. In addition, the Court cited the responsibility of the Director of Central Intelligence for protecting intelligence sources and methods as stated in 50 U.S.C. 403 (d)(3). The CIA Secrecy Agreement was viewed as an effort by the Director to comply with his duty.

However, it is clear that there is a limit to using security classifications to restrict the dissemination of information. The Court indicated that a classification should equate with a real need for secrecy in the conduct of national defense. One member, Judge Craven, favored judicial action to assure elimination of frivolous and absurd classifications. Also, the Court made the point that a person cannot be denied the free use of information bearing a classification marking if it has been published. The CIA Secrecy Agreement stands with Court approval as a model for secrecy commitments by Federal employees. But its longevity evidently depends on *effective classification management.*

The CIA Secrecy Oath contains a promise by a person separating from CIA employment that he will never disclose *any* information relating to national defense and some other CIA matters without written consent. The Fourth Circuit Court of Appeals ruled the Secrecy Oath to be unenforceable. First, it is not a contract, since there is no consideration. Second, to the extent that the oath purports to prevent disclosure of unclassified information it "would be in contravention of the individual's First Amendment rights"

The Department of Defense secrecy form for contractor employees, Defense Supply Agency Form 482, contains three significant points.

- First, the brief statement about secrecy that is signed upon employment and also upon separation reads: "I shall (will) not knowingly and willfully communicate, deliver or transmit, in any manner, classified information to an unauthorized person or agency." That secrecy statement, of course, is not a contract. There is neither a second party nor any consideration.
- Second, there is the moral aspect of the secrecy statement. It appears to be a firm personal commitment for secrecy. But, as a simple fact of life, a person may in good conscience, with no qualm whatsoever, exercise judgment—
  - As to whether a specific item of information "could reasonably be expected to cause damage to the national security," particularly one

with a frivolous or absurd classification as referred to by Judge Craven, or

- As to whether a prospective recipient is "an unauthorized person or agency." In comparison, the CIA Secrecy Agreement is reasonably limited to certain CIA information. And the controlling factor on disclosure is in terms of duty performance, not the questionable, loose terminology of "unauthorized person or agency."

- Third, DSA Form 482 seriously misrepresents the Federal Criminal Code by falsely informing people that if they should "knowingly and willfully communicate, deliver, or transmit, in any manner, classified information to an unauthorized person or agency, ... such improper disclosure may be punishable under Federal criminal statutes."

That misrepresentation is compounded by erroneously referring to those portions of law reproduced in the DoD Industrial Security Manual as "relating to the safeguarding of classified information." In truth, there is *no* law in this country making it a crime for an individual to disclose information to another person because of its bearing a classification.

None of the ten subsections of the espionage laws, 18 U.S.C. 793 and 794, as reproduced in the Industrial Security Manual uses the term "classified information." None of the other reproduced statutes refer to "classified information" except 18 U.S.C. 798, which applies to certain cryptographic and communications intelligence matters. The law would be the same without the word "classified."

As a matter of judicial history, the Federal District Courts, the Circuit Courts, and the Supreme Court accorded the Top Secret classification no standing at all in the *New York Times-Washington Post* case involving the Pentagon Papers.

In the Marchetti case, neither the CIA nor the courts reflected any concern about his already having given classified material to *Esquire Magazine.* CIA only took civil action in the case to have Marchetti comply in the future with his contract for secrecy. The Agency did not misrepresent the law and initiate criminal action as the White House did in the Ellsberg case. As for Dr. Ellsberg, it has been pretty well confirmed that the indictment for his handling of some old documents marked Top Secret was a purposeful political attack. It was hurriedly and falsely drawn from what people now call a fetish for security classification and secrecy.

During the Ellsberg-Russo trial, the prosecutor introduced into evidence the copies of DSA Form 482 that they had signed as RAND Corporation employees. An attempt was made to show that, on the basis of those signed statements, the defendants knew that they had committed a crime. But the Court's rulings pursuant to actual law, the true law, stopped the effort. It was clear that DSA Form 482 was more of an embarrassment than an aid to the prosecution. (Reference: Trial Transcript; pp. 20,010-20,014, *et. al.*)

The prosecution team obviously tried to make an example of Dr. Ellsberg at any cost. Among the indictment documents which the RAND Corporation had given him, and he had returned in good order, were 11 that were still classified Top Secret when the trial began, last January. The Departments of State and Defense had refused to declassify them. But the prosecutor introduced all 11 as evidence in court anyway. There, they automatically became and still are, *public records.* They are Top Secret public records, if you can imagine such a farcical Gilbert and Sullivan contradiction. (Reference: Trial Transcript; p. 9295) My point is that Dr. Ellsberg was tried for having permitted one person to have access to seven of those 11 documents, a second person to have access to one of the same seven, and a third person to have access to another of the same seven. But no one in the Executive Branch was indicted for disclosing those seven Top Secret documents, plus four others, to the general public. Based on observation and many personal contacts, I believe that mismanagement of classification policy and the misrepresentation of law, such as is reflected in DSA Form 482, have contributed much to the deterioration of Executive Branch credibility as it exists today.

Among those actions which this Society could consider to restore trust in the classification system is a recommendation to the Secretary of Defense that DSA Form 482 be eliminated. Truthful representation of the classification system is both a legal and moral obligation of the Executive Branch. It is also an essential element of communication in any effort to improve classification and declassification management.

Elimination of DSA Form 482 would, of course, negate the restriction published in Item Q, Appendix I (One) of the DoD Industrial Security Manual against contractors using "local forms." A contractor should be free to ask his employees to promise in writing to help him comply with contractual obligations for safeguarding classified information.

Assuming that DoD would want a model security agreement to assure some degree of uniformity, this Society could recommend one for such use. It could be the type of agreement that I have prepared and shown as figure 1.

The employee would promise, as a condition of employment, to:

- Adhere to contractual requirements for safeguarding classified information to the extent that they are made applicable to him in the performance of his duties, and not disclose such information to any person except as authorized by the contractor.
- Advise the person designated by the contractor if a question arises regarding either the authenticity of an assigned classification, or the practicality of maintaining an assigned classification in relation to requirements for disseminating the information involved.

Those are my suggestions to the Society to assist in accomplishing its stated purposes, now and into the 1980s. ■

NATIONAL SECURITY INFORMATION SECRECY AGREEMENT

Employees and Consultants of _____
(Name of Contractor)

_____
(Date)

I understand that _____ *(NAME OF CONTRACTOR)* _____ has entered into certain contract(s) with the United States Government, under which the [contractor] *agreed:*

1) To be responsible for safeguarding all official information under the [contractor's] control which relates to the contract(s) *and* which the Government *has* (a) designated as requiring protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (collectively termed "national security") and (b) classified as CONFIDENTIAL, SECRET or TOP SECRET.

2) To assure that an item of CONFIDENTIAL, SECRET or TOP SECRET official national security information is disclosed or furnished only to (a) the [contractor's] employees and subcontractors who require access to such information in the performance of tasks or services essential to the fulfillment of the contract involved, and (b) such other persons as the Government may designate.

3) To inform employees engaged in work involving access to CONFIDENTIAL, SECRET or TOP SECRET national security information of their individual responsibilities for safeguarding such information.

IN ORDER THAT THE [CONTRACTOR] MAY FULLY CARRY OUT ITS OBLIGATIONS, AND IN CONSIDERATION OF MY EMPLOYMENT, I HEREBY AGREE THAT I SHALL:

1) Adhere to the contractual requirements for safeguarding CONFIDENTIAL, SECRET and TOP SECRET national security information to the extent that the [contractor] makes those requirements applicable to me in the performance of my duties, and shall not communicate such official information to any person except as authorized by the [contractor].

2) Advise my immediate supervisor or such other person as the [contractor] may designate if a question arises regarding (a) the authenticity of an assigned CONFIDENTIAL, SECRET or TOP SECRET classification or (b) the practicality of maintaining an assigned classification in relation to requirements for using or disseminating the information involved.

_____ WITNESS

_____ SIGNATURE OF EMPLOYEE

(This agreement form was drafted in July 1973, by William G. Florence, Washington, D.C., for use by any person interested in promoting the United States national defense.)

FIG. 1

CLASSIFICATION AND FOREIGN MILITARY SALES

Mr. Edward Silver,
Hughes International, Hughes Aircraft Corporation

Mr. C. C. Fredericks,
Westinghouse International, Defense and Public Systems Corporation

Mr. Leonard A. Alne,
Director, Sales Negotiations
Defense Security Assistance Agency

Mr. Silver: What I'm going to talk about is probably quite unique, because up to now, everything that has been said has related to the protection which is accorded material specifically marked as requiring protective handling. Dealing on an international basis, we find that there are limitations on the disclosure of material which carries no markings at all. This is the so-called "technical data," and what qualifies as technical data is basically left up to you to determine. So you see this is a different type of security game that we are in.

To begin with, I think that we all want to avoid security problems, especially when they are problems with classified material, with overseas operations or when they involve our best customer, the Department of Defense.

I think our biggest problem today in security from an international sense is that the program is basically the same today as it was over ten years ago or when it was conceived. During this period of time, there have been many changes in the marketplace. Some of these include: Many international suppliers where there used to be only a few, and I mean suppliers from both the United States and abroad. No longer do the foreign customers look to only one contractor and they are no longer interested in turnkey systems. Today, they are more interested in equipment that is designed for their needs rather than the needs of the U.S. military. Many of these countries have requirements and tactics that are different from the United States. Also the countries today insist on an implantation of technology. If you're going to get their money, they expect to get something in return that is going to raise their level of technology. They are also interested in something called offset procurement. Not only do they want to build up their industry in technology, but they require some dollars flowing into their economies.

We also find a new interesting concept called reverse licensing. Until recently, I don't think anyone in the United States would have ever thought, that for a U.S. military system, we would go abroad and license the production in the United States. Today, this is a fact of life and some of this information has both U.S. and foreign classifications.

There has always been the complaint by U.S. contractors that the foreigners have some inroad, by which they can accomplish things faster and easier than we can when satisfying government requirements.

These are all developments that have happened since the original concept for international security was designed. Today, we also find that when the U.S. Government's security requirements changed, they became more complicated. In addition today, we face a dollar crisis overseas. These things adding together mean that we must be more aggressive in our marketing and we must be provided the tools for a more contemporary international security program.

In order to do this, we should ask ourselves four questions as shown in figure 1.

1. IS EVERYTHING WE ARE DOING NECESSARY?
2. IS THERE A BETTER WAY?
3. HOW CAN WE CHANGE?
4. NOT, WHY WE CAN'T CHANGE.

FIG. 1

Too many times when we are dealing with governmental bodies, we come to the conclusion that we're doing something because it can't be changed, i.e., because there are so many organizations involved that a change is impossible. But for right now, I would like to capture your imagination with the idea that change is possible. Let's proceed in that direction.

Basically, to make any program work, all parties involved must have commonality in purpose, direction, and control. The international security program today has many overlapping uncoordinated controls. We seem to find that each of the organizations I have listed in figure 2 here feels it is the last bastion for protection of the United States' defense and therefore, it has responsibility for U.S. foreign policy. Every one of these organizations seems to have a different idea of what the defense requirements are and how to implement them. There is no commonality of purpose, even though there are many regulations. These regulations seem to be interpreted in as many different ways as there are people interpreting them. I'll show you a few examples as we go on.

In order for a program between industry and Government to work, I think we have to establish an understanding and mutual trust. In order to do this, we have to develop joint goals common to both industry and Government. I think that it is becoming more evident, both to industry and Government, that we have a common goal today which is to increase our foreign sales thus helping the dollar crisis.

Here are some of the things that I'm proposing: That we come up with some central program approval that is recognized by all organizations. As an example, we have experienced situations where we have had foreign representatives come to one of our plants for classified discussions and tours. Even with the visit having been approved after over 30 days of staffing, we still face the idea that whenever there is a disclosure of classified information, the disclosure can only be on the basis of a Government-to-Government transfer. Thus, a representative of the U.S. Government must constantly be present. That is, we arrange our disclosure schedule to the work schedule of a Government employee. This is not the intent of the program as I understand it. The intent of the program is that once a visit authorization has been established and the need-to-know has been determined, the contractor is allowed to give briefings on an oral-visual basis, but no classified documentary releases. This is the rule of Government-to-Government disclosure and it applies only to documentary releases.

Another example is a requirement that foreigners must have a security clearance authorization to tour unclassified manufacturing facilities even when no "technical data" as defined by the Office of Munitions Control (OMC) is involved.

Again, it's not in the regulations. There is no apparent reason for it other than we happen to have a plant representative who has made this determination. If the foreigners don't have a security clearance, they're not going to get into this facility.

Different levels of clearance. Occasionally, we will have a mixed group of foreign nationals visiting our facilities some from industry, some from government. The authorization for the government representatives permits classified disclosures; for the industry people representing the same government, "no classified disclosure authorized." What does the contractor do? It's very embarrassing and confusing for us, as well as for the visitors. In the end, we feel that foreign industry and government visitors jointly critique their visits, freely exchanging notes. These artificial barriers only confuse all parties and accomplish nothing worthwhile. Not only is it left up to industry to promulgate this distasteful withholding of information, but we are slapped with a regulation telling us we can't divulge to the foreign nationals what their level of disclosure authorization is, thus preventing prior coordination to determine, should we either not have the visit at all or defer the meeting until a meaningful disclosure level is granted.

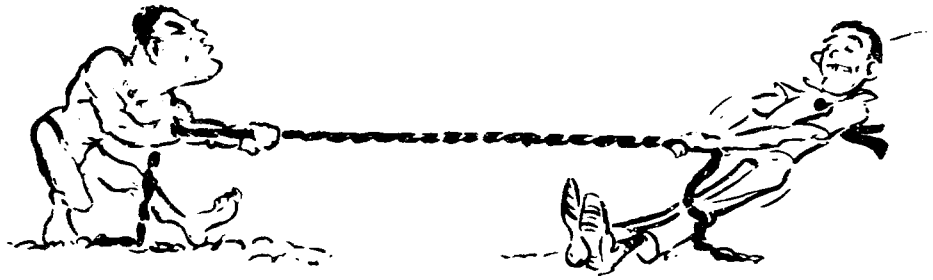
This next example is comparable to riding on two horses at the same time. Under the existing regulations, if you hold a DSP-85 license for the disclosure of classified information, you can use it as the basis for establishing a classified visit authorization overseas. We are then permitted to go overseas and carry on discussions of U.S. classified with foreign nationals. When these same foreign nationals come to the United States, it's not the State Department that has cognizance, but the Department of Defense. The Department of Defense staffs a determination as to what access these same foreign nationals are going to have when they visit our plant. This is provided to us in the form of a visit authorization.

There is no continuity between these two disclosures. We have had numerous occasions where for several years, we have held DSP-85s, and on this basis, we have exported classified documents to foreign nations. In some cases, the foreign governments have even bought the classified system and have it in their possession. They send their technical people here to talk to our technical people and we get an unclassified visit authorization.

We have a problem in sending classified briefing materials overseas. Just because we have an export license, only means we can export the material. The placing of classified support documents in MAAGs is still at the discretion of the Contracting Officer.

Today, in order to get a classified document reviewed by the Department of State for foreign release, we have to have the Contracting Officer's approval for its publication. If you change the document or modify it in any way, you've got to go back to the Contracting Officer again, get his approval and in turn, go back through the whole chain of review and authorization. What I'm suggesting is, once a Department of State approval has been obtained for the release of a certain level of classified information, a plateau has been reached and you don't have to go back to the Contracting Officer or the Department of State until you are ready to go to a higher plateau. This case-by-case review by the Contracting Officer is quite a problem to us and it seems to be a complete duplication of staffing. First, we go to a Contracting Officer, get his permission to publish a classified document, and then send the document to the Department of State. The Department of State doesn't make a determination itself. It sends the document to the agency or activity that was involved in the procurement of the overall system, and so the document goes back to the same contracting activity that authorized its publication a few weeks earlier, which is just a redundant step.

INTERNATIONAL SECURITY PROGRAM



NEEDS: COMMONALITY IN PURPOSE, DIRECTION, AND CONTROL.

HAS: MANY OVERLAPPING, UNCOORDINATED CONTROLS BY:

A. STATE DEPARTMENT.

B. COMMERCE DEPARTMENT.

C. DCAS.

D. DCASR OFFICES AND INSPECTORS.

E. THOUSANDS OF CONTRACTING OFFICERS.

F. GOVERNMENT PLANT REPRESENTATIVES.

G. MILITARY SERVICE CONTRACT MANAGEMENT ORGANIZATIONS.

H. MILITARY SERVICE FOREIGN SALES.

I. MILITARY SERVICE FOREIGN LIAISON OFFICES.

J. MAAGS, MDAOS, AND MILITARY ATTACHES.

K. CUSTOMS.

FIG. 2

I would like to further amplify this point by drawing attention to the confusing instructions provided, as to why, and what the Contracting Officer is reviewing the document for. I've heard that the review purpose is to determine the correctness of the security classification, but I have never seen this in writing and the logic of checking the classification both before and after submittal to the Department of State escapes me. Our suggestions and a few additional points are found in figure 3.

This approval that requires an annual renewal (for classified) from the OMC, doesn't really unlock all the doors as far as all the organizations listed in figure 2 are concerned. It doesn't really give you a basis for having visitors come into your facilities for the disclosure of classified information. It doesn't really seem to cut the red tape of Contracting Officer approvals. It only seems to apply to your activities with foreign governments overseas, not in the United States.

I would like to see established some basis like the license from OMC which would permit us to immediately place classified documents relating to the approved program in various MAAGs and embassies overseas for the use and support of our marketing efforts. At the present time, we have to go to the Contracting Officer to get this permission. Our suggestions are contained in figure 4.

Further, I would like to see Overseas Security Eligibilities (OSE) abolished. OSE is something that has been with us for ten years, and apparently the only reason we have it is because no one has any imagination as to how to get rid of it.

About the only thing it does is deny access to "no foreign information." From what I understand, industry people are probably not supposed to have such information anyway because this is basically intelligence information. The other prohibited areas of information are already eliminated from disclosure to overseas personnel by a lack of need-to-know.

The OSE is only issued for two years. Every two years you go through the paper reshuffle, having the overseas employee reconstruct, read, and sign a bunch of forms. Because these employees are doing this operation thousands of miles away, you can only hope they fill in and sign all parts correctly including the privacy portion.

Connected with this is the problem that you are sending out visit requests to foreign governments generally for an extended period of time up to one year. If the OSE expires in the middle of one of these terms, we find that DISCO doesn't know exactly what to do. Should they certify the individual's clearance only for the period that the OSE is to run, or should they strike his name off the list. So the fact that the clearance is going to expire every two years presents a problem when you're establishing term clearances overseas.

One other point on OSEs is in the case of our people in Canada and the Far East, I don't know why we have to have an OSE. The main idea of the OSE, of course, is to establish a record for the Office of Industrial Security, Europe (OISE). Obviously, OISE is a little bit out of touch with what is going on in Canada and the Far East.

On another matter, I would suggest that we provide more realism in handling foreign classified information. When restricted information comes to the United States, we protect it as Confidential. This is kind of an absurdity if you have ever dealt with any foreign nationals, because you know they send restricted information through first class mail, hand carry it in briefcases, and store it in desks and wooden files. The minute we get this foreign "For Offical Use Only" information in the United States, it's into one of those GSA file cabinets, and we go through all the procedures that are followed for U.S. Confidential material.

Swedish Confidential (or Hemlig) creates another problem in that it translates to something in between Secret and Confidential, depending on who is doing the translation. You will probably end up with a Secret document that will be in your accountability records forever for it is excluded from downgrading review.

I don't know if you have ever had any experience in preparing DD 254s involving a foreign classified contract. The problem is, who approves a DD 254 for subcontracting based on a foreign classified contract? Our normal response is that you send your DD 254s to the Contracting Officer for approval. When dealing with a foreign contract, who is your Contracting Officer? In any case, he is probably overseas and knows nothing about security requirement check lists. When you try to get him to approve your DD 254, you have entered into a long chain of events. Generally, by the time you get an approved DD 254 back through the official Government channels, you'll find that the subcontract was awarded and has long since been completed.

I think that the contractor should be given authority to sign off on DD 254s for foreign contracts. We know as much about what's classified as the foreign contract adminstrators do. That's on the basis generally that we have been told what's classified, which is usually only orally. Foreigners don't seem to appreciate the fact that they have to write DD 254s and furnish some type of written guidance on an annual basis.

Retention requirements. Since DD 254s and all of these requirements are good for U.S. classified information, obviously they must be good for handling foreign classified information—they are not. They don't work. These points are summarized in figure 5.

Being from California, maybe I appreciate the Hearst Castle more than you do. But if you have never seen the Hearst Castle, let me assure you that it is something marvelous to behold. Each room is like a museum. It's breathtaking to see it. The only thing is that none of the rooms tie together. Figure 6 establishes a relationship.

I liken this to our industrial security program for international operations. It works. Unbelievingly, it works. But there's no continuity in the whole program. There is no overall design or carrying on from one organization to the other. It has organization by organization independence. We ought to be able to do better than that in this important field, especially if we're going to be around in this arena in the 1980s.

Mr. Fredericks: I am from Westinghouse and I have marketing responsibility for all of our activities in the international or export world, and I'll make my comments strictly from a marketing standpoint. I want to talk about your subject, classification. I want to expand that into releasability which is a function of the Department of State (known as the International Traffic in Arms Regulation (ITAR)). And very frankly I want to make these

ELIMINATE DUPLICATE PROCESSING AND CONTRADICTORY POLICY.

1. ELIMINATE CASE–BY–CASE REVIEW BY CONTRACTING OFFICERS BEFORE REQUESTING DSP–85 LICENSE. CONTRACTING OFFICER REVIEW IS ILL–DEFINED AS TO PURPOSE AND IS A DUPLICATION OF PROCESSING:

a) ISM 5p REQUIRES PUBLICATION AND DISTRIBUTION AUTHORITY.

b) DSP–85 REQUIRES REPRODUCTION AUTHORITY.

c) 22 CFR 125.21 REQUIRES "TREAT AS REQUIRED".

d) WHY DOES CONTRACTING OFFICER REVIEW DOCUMENT?

e) WHAT IS HE REVIEWING DOCUMENT FOR?

f) HOW MANY CONTRACTING OFFICERS KNOW THE ANSWER TO THIS?

g) DO CONTRACTING OFFICERS FEEL THEY HAVE RESPONSIBILITY FOR NATIONAL DISCLOSURE DETERMINATIONS?

h) AFTER DENIAL ON THE CONTRACTING OFFICER LEVEL, WHAT IS CHANNEL OF APPEAL TO LEVEL OF GOVERNMENT MAKING FOREIGN POLICY?

i) WHAT DOES THE CONTRACTING OFFICER'S ENDORSEMENT OF A DOCUMENT IMPLY?

FIG. 3

2. ELIMINATE CASE–BY–CASE DOS REVIEW.
   a) ONE "IN PRINCIPLE" REVIEW OF STUDY, DATA, HARDWARE.
   b) APPROVE ON BASIS OF EQUIPMENT CAPABLE TO ACHIEVE CERTAIN LEVELS OF PERFORMANCE.

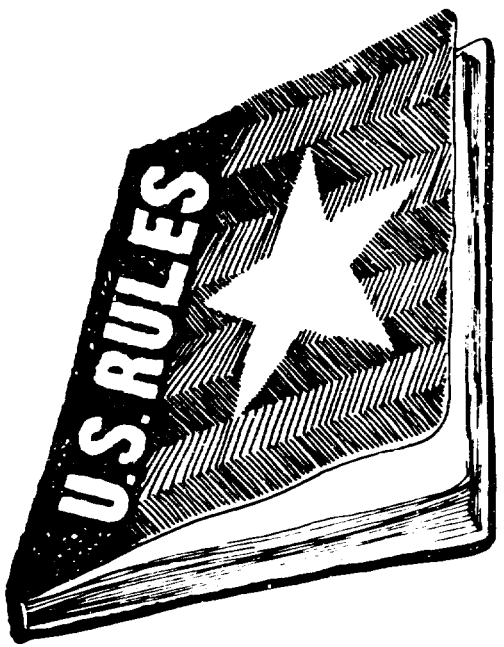
3. ELIMINATE ANNUAL CASE RENEWALS FOR DATA RELEASES.

4. OMC APPROVAL SHOULD AUTOMATICALLY PERMIT CLASSIFIED FOREIGN VISITS TO U.S. FACILITIES FOR DISCUSSIONS OF SUBJECT MATTER.
   a) ONLY OTHER REQUIREMENT SHOULD BE CERTIFICATION OF A PERSONNEL SECURITY CLEARANCE BY SPONSORING GOVERNMENT.

5. OMC PROGRAM APPROVAL SHOULD AUTOMATICALLY AUTHORIZE CLASSIFIED TRANSMITTALS TO MAAG/EMBASSIES OF RELATED MATERIAL FOR BACKGROUND BASE.

FIG. 4

INAPPROPRIATE APPLICATION OF U.S. RULES TO FOREIGN INFORMATION.



1. RETENTION REQUIREMENTS SAME AS FOR UNITED STATES.

    a) FOREIGN GOVERNMENTS CANNOT APPRECIATE NEED FOR REQUIREMENTS.

    b) AUSTRALIA REQUIRES RETURN (NOT DESTRUCTION) OF ALL MATERIAL FURNISHED UNDER PRECONTRACT NEGOTIATION.

2. ANNUAL CLASSIFICATION GUIDANCE.

    a) LUCKY TO GET ANY WRITTEN GUIDANCE.

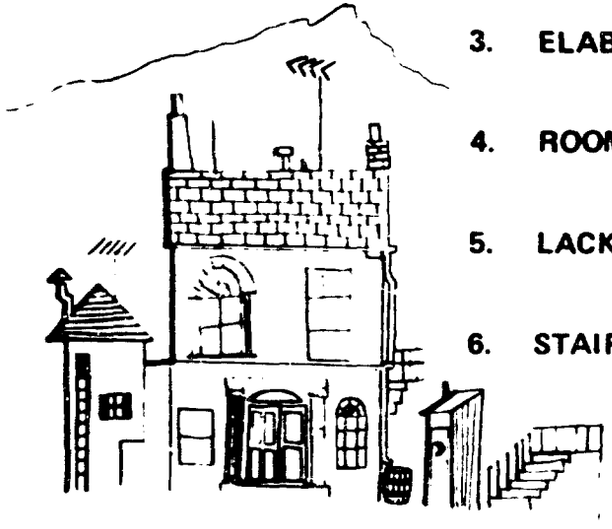
3. APPROVAL CYCLE FOR SUBCONTRACT DD–254's.

    a) GENERALLY SUBCONTRACT COMPLETED LONG BEFORE APPROVED DD–254 RECEIVED.

    b) PRIME CONTRACTOR SHOULD BE AUTHORIZED TO SIGN THESE FOR FOREIGN GOVERNMENT.

FIG. 5

IN SUMMARY, THE PROGRAM IS COMPARABLE TO THE HEARST CASTLE.



1. ARCHITECTURE NOT CONTEMPORARY OR FUNCTIONALLY ORIENTED.
2. NO OVERALL CONTINUITY IN THEME.
3. ELABORATENESS WITHOUT PURPOSE.
4. ROOM--BY--ROOM DESIGN INDEPENDENCE.
5. LACK OF CONTINUITY IN OVERALL ARCHITECTURE.
6. STAIRWAYS THAT GO NOWHERE.

FIG. 6

comments in the context of how can I avoid the impact of classification and releasability; and lacking that, how can I minimize that and yet get on with my real purpose in life of accomplishing sales in the international market? So if you will bear with me, these are some of the things I'd like to bring to your attention.

In the first place, I want to comment on the sometimes over-used expression of communication, but if you will, imagine the sort of things that you have discussed here the last couple days and that we have brought up during this particular session, and if you can imagine how they all might impact upon American missions located outside the country for a variety of reasons including those who are expected to provide assistance in some manner to people like myself in the accomplishment of foreign sales in the military market, and if you can imagine their ability then to understand and work their way through the various policies, procedures, and maybe even strategy as it impacts upon what they have to do day-by-day and what they are asked to do by people like myself when I show up in the country and say I'd like to do thus and so. This then emphasizes why communications are very important.

And just to share with you a situation that occurred very recently, I was in a foreign country making such a request and in doing so the response was, Gee, I haven't really gotten those instructions back through my own channels; could you help me in getting those instructions? Of course, I'd like to. When asked how I could explain it, I did, and I cited the authority that I felt existed for my particular approach to it. But I did encourage him to go back through his own channels and seek guidance in his own way because I really felt that unless he knew what his instructions were in that particular matter that he wasn't going to be particularly comfortable in doing the sort of things that I thought I needed some assistance on, and it did impact and impinge upon classification and releasability. I was asking for help in accomplishing a sale where my primary competitor is a foreign contractor.

I'm not being critical when I say it. However, I think—I'm acknowledging that it is a very complex problem for all of us especially we who operate on the fringes of this. We look to our experts to keep us honest if you will so that we know when we may be going astray, but our primary purpose is to accomplish sales and yet conform with the security requirements.

Another area that has been of concern to us involves technical assistance agreements or license agreements that we extend to people, for a variety of different reasons, who are located outside the country. In doing this we obtain from the Office of Munitions Control their approval of our technical assistance agreement and they have a prescribed manner by which we submit information to them for approval. And their approval then is made on the basis of inputs that they get from people at DoD and other places. Once it's approved we would think that we have a vehicle that will permit us to act upon the technical assistance agreement. We have usually collected a fee for this information that involves proprietary data on our part and it does have value, and so we're quite concerned about protecting our own continuing proprietary rights in it.

But we do have an obligation inherent in the agreement to provide information where there are engineering changes, and in the most part we find that we are able to provide this changed information or new information from time to time and can ship it against the technical assistance agreement that the Department of State has approved.

However, from time to time we find that that is not the case and we think it stems from the fact that there isn't a clear understanding between the Office of Munitions Control and the DCASR as to how we are obliged to transmit that information.

Where it's classified, it does go through Government channels. The Office of Munitions Control takes the rather broad viewpoint that whenever there are changes involved these are submitted through the established channels as long as it does not go beyond—that is as long as it's within the limitations of the original agreement they approved. The DCASR does not always agree with this and from time to time there are occasions where we are obliged to go back and seek and obtain a separate license to ship this revised information.

This is expensive, it's time consuming, it delays the receipt of the information by the customer. It delays the receipt of payment from the customer. There are a whole host of reasons as to why this is a burden on industry and we believe that this is an area where further coordination is required by more than one element of the Government in order to relieve us of this extra burden.

We have always found a way. We're never stopped dead in the water. We don't find this to be insurmountable, and we have found a way to get around it. But in so doing it's time consuming and it's expensive. We don't like it. We'd like to see it changed. So I bring it to your attention today because it does impact negatively on our ability to perform against contracts and that's always remembered the next time around.

There's another aspect of the same thing and it really concerns the transmittal or dissemination of classified information to foreign nationals. I'm talking now about foreign nationals who are natives of a country where there is an ongoing negotiation to buy a piece of equipment that may not be classified but some of the data may be classified.

We are not able to make use of the facilities and services of these people because we just can't disclose this information to them. However, some of these same people do have security clearances of their own country, the very country who is buying the equipment from us and ultimately they do have access to this information, but we're not able to cause them to have access to this information in such manner that it might be beneficial to us in our sales objectives.

We understand the rationale as to why this is the case, but nevertheless it seems to be a bit inconsistent for it to happen this way. I wanted to bring this to your attention.

A third area that offers some concern to us involves some of the things that we and the industry are doing today that result from our own initiative. I'm talking now about the development of systems that in the main are oriented to the needs of the international market. Right now we don't anticipate a need on the part of U.S. military services and they may never be in U.S. military services inventory, so here we're dealing with a number of differences.

In the past most foreign military sales have been made on the basis that the system was previously developed on a contract from the U.S. Government and applied by one of the military services and thereby was in the inventory. And in being carried out in that manner we had a contracting officer, we probably had a project officer, from either of whom we could seek guidance from time to time, and we had a DD 254. And while some of the earlier comments spell out some of the problems that this represents it did offer us guidance and assistance in our ongoing efforts.

In the situation that I speak of now, none of these exists. We're doing it on our own initiative, at our own expense, it's a private venture type undertaking. We don't have a contracting officer, we don't have a DD 254, but yet we have a need to conform to classification requirements and we have a need to conform to the "eye tower" requirements about the release of technical data.

Once again we're not dead in the water. It's not insurmountable, but we find that as we go from place to place seeking guidance, guidance that has been recommended to us, you know, we find that we come up with conflicting information and we walk away perhaps sometimes more confused than not. But in the final analysis we do find a way to overcome some of these problems and get on with our job.

To help you better understand what some of these systems are, you may be familiar with the concept that DoD has for looking for initiative whether on the part of the aerospace industry or private industry, if you will, as to a better way to meet a given requirement and also have the design-cost concept. So these very criteria make these systems fairly attractive in the international market because these are some of the things that foreign governments are concerned about as well.

So this is a situation that we face. The ITAR when it was originally outlined or set up did not anticipate this sort of thing, and we find ourself trying to do business in an environment of change but working with ground rules that are 10, 15, 20 years old. These continue to pose problems to us but they don't stop us. We do forge ahead.

Well, in summary these are three areas that I wanted to share with you, to indicate the sort of impact that classification and releasability have on industry's objectives in realizing sales in the foreign market.

I'd like to close then in offering a couple of conclusions that in my mind might help the situation.

The first is to decontrol and declassify wherever possible and as soon as possible, very expeditiously. These sorts of things are happening, I know, but they usually happen too late to enhance the system's salability in the export market. Because it usually takes place so late in the scheme of things that a foreign government is looking for something a bit more advanced than what we are able to offer under these conditions. I do think it's a viable consideration to think of decontrol and declassification as soon as possible.

The second thought concerns the sort of situation that exists where high technology products for the international market have to be considered in terms of rather complex national security and foreign policy considerations. This being the case there are a number of constraints on the Munitions Control Office as to what they are able to release.

I should quickly say that they have been very cooperative with the industry as a whole by providing guidance in principle as to what may or may not be released to what countries, but this is only just a measure in principle and is not particularly definitive in the way of direction.

The follow up to that is an application for releasability and sometimes that's very time consuming, and after a great deal of effort we may find out that the thing we would like to release and sell to a foreign government is not in and of itself releasable. So what I'm really talking about here is the time and effort industry expends in planning the sales program only to find a product that we would like to sell is not in the final analysis releasable.

And the thought I'd like to leave with you in this respect—and we and other people in industry have expressed this before—but releasability in large part depends upon the DoD interpretation of the national disclosure policy. This is a classified document, thereby not available to industry per se. So I am suggesting as my second recommendation that in some way or another the policy be reviewed with industry, classified briefing, if you will, but provide us this information so that we in turn can put our resources where there is a likelihood that releasability can be realized and thereby be more effective as an industry and help perhaps in so doing redress the balance of trade and balance of payments problem.

So I'd like to leave those two thoughts with you.

Mr. Alne: I confess to some dilemma. I don't know whether I should talk about something I know something about like foreign military sales, which I suspect doesn't interest this group very much, or to try to talk about something which does interest you about which I know very little, namely, classification; but concerning which I have come to some visceral conclusions this morning and I am sorely tempted to talk about that which I know nothing about. But I'm a longstanding bureaucrat so I suppose I'll take the easy way out and talk about what I know about under the assumption that you are interested in foreign military sales.

In fiscal year 1973 we took orders for just short of $3.4 billion; that's through the Government-to-Government channel; and another $0.6 million through the commercial channel for a total of $4 billion. Four billion dollars in orders in this business I think is about half of what we exported in all agricultural products in the same year. That was before the sale of wheat to Russia. The data may be different next year.

Now, these orders represent a very complex business that involves a lot of people.

We sell a lot because the world is buying a lot and because the United States, even though the world is changing, is a major source, unavoidably a major source, of much technology that now is reflected in military equipment.

We began very austerely in the early 50s with legislation which authorized the U.S. Government to sell military equipment under the control of the Department of State on those occasions when countries wanted to buy it. At that time the whole country was much preoccupied with the need for grant military assistance. It became known as grant military assistance or mutual security or

whatever you want to call that program, under which we accumulated grants of military equipment abroad of about $38 billion—most of that in the 50s. The program trailed off by 1960 into much smaller levels of grants. Correspondingly the level of sales went up. The plot of sales crossed the curve of grants in September 1962.

The grant level now is less than a billion and something more than half a billion depending on which Congress operates on which legislation. The level of sales is running about eight times as high.

This came about because it became evident in about 1960, first, that countries could pay their own way, and, second, that the United States began to experience a very serious imbalance of payments. Mr. Kennedy told Mr. McNamara in that year, I want you to do two things; I want you to reduce the cost of U.S. forces employed abroad—and indeed Mr. McNamara took that $3 billion theretofore prevailing and reduced it to about $2.6 billion; that's in annual foreign exchange expenditures of the Department of Defense; until about 1965 when Vietnam came to mask all of our data, and no longer does anyone follow, I think, exactly what our costs are.

Then he said, the second thing I want you to do is to offset as much of the remaining cost as you can with payments from countries who can now afford to pay for their equipment as opposed to getting it free under grant equivalent.

That began what you might call a formal sales program. I dislike the word program because it takes two to buy and sell. I don't know how to program a sale at all. We do have a set of sales activities that have many aspects to them and, as I say, total quite substantial numbers.

I should be able to report to you how I could double or triple those sales if I didn't have all the problems of classification and control of information and control of disclosure and everything that occupies this group. Frankly, I haven't been too aware of the difficulty.

What I have learned this morning is that we in Government are apparently forcing U.S. industry to go through an enormous amount of avoidable and self-inflicted nonsense in order to make the sales that they do.

I don't know why this is happening. I really couldn't believe it is happening. But I have to accept what my colleagues on the panel say. It must be because what began perhaps centuries ago as a valid observation, if you're in combat in the middle of the night and you want to surprise the enemy in the morning by coming around a certain corner where he doesn't expect you, don't send a runner in the middle of the night to tell them where you're going to go.

That makes good sense. You withhold from your enemy that which he shouldn't know and that which is in your interest to withhold from him.

Well, if that was valid, I suppose the next embroidery on that valid rule began a couple centuries ago and since then has grown into the elaborate and contrived and I suspect ludicrous accumulation of rules under which we actually now make industry act differently than Government.

I don't know how you're any different than we are. Take any one of us, Government or industry now, we all have the same levels of responsibility. Why we have to have this—I heard this morning a Government official sitting in a room while the man who knows what he's talking about conveys to the man who wants to know and is allowed to know—why that Government official sits there listening to a conversation that he cannot control and probably cannot understand is beyond me. In any event, it's manifestly inefficient. And why we distinguish between citizens in the United States and citizens when they go abroad, I don't know.

So I am tempted I must say to search for an Emil Kratzig. I thought of him this morning. He's the subject of a story by Ludwig Bemelmans called *Sacre de Printemps*. I think it might become the story or the novel or the literary basis for the, I think valid, complaints of this industry.

The story is about a mythical country in Europe that oversystematized its form of government. It's a satire on the development of Nazi Germany. But it goes on at some great and fascinating length describing how they have in that government a Department of Seasons for the sole purpose of managing the seasons. There are subdivisions for Spring, Summer, Fall, and Winter.

In that country every man that's born is given a civil service classification and thereafter his entire life is determined, whether he's from Class 1 which is the very blue-blooded top or down to Class 6.

This organization prevails throughout all sectors of the economy. If you are Class 1 and you die you get a certain kind of funeral. It involves a huge orchestra, a complete choir; you get gold-plated harness on eight horses pulling enormously convoluted hearses—well, it describes it in great length; I haven't read it for years; I'm sorry I can't give you all the bibliography involved here. But if you're second class I remember you have only silver buckles on the harness; you only have four horses instead of eight; you have a small choir instead of a complete orchestra. If you're third class it goes down to a quartet. And I do remember sixth class, the lowest class of all; that's where you have a little box with a hook on each side; two men carry you and drop the body into the grave and reuse that coffin.

It describes transportation. If you're first class you can imagine what kind of a conveyance you are allowed to ride in all by your magnificent self. Then it goes on down where if you're fourth class I think you're in carriages with pine seats. I do remember sixth class. There is no floor in that car. You run along the tracks.

Everything is marvelously organized and everyone believes in it. Everybody was born into that system. And although it must look ludicrous on occasion to see someone running along the tracks, that's how it is in sixth class.

Well, in this system, what makes the drama, what makes the tension of the story is that there is one man who does not follow the rules. Everyone else who didn't follow the rules promptly had his head chopped off but this is the last one, Emil Kratzig, the last non-conformist. And the government kept him around because he was kind of a reminder. No official could really bring himself to do away with that last remnant of the old world.

Well, Emil Kratzig, for example, did not change from winter clothes to spring clothes promptly on the first day of spring notwithstanding the rules of the Department of Spring. If it was a nice day he put on spring clothes earlier.

Well, he did that one time and he guessed wrong. He caught a cold, because he had his light clothes on too early. The story goes on in that vein, describing I think in a different sequence than I did the whole context. But in the end there is an officer Umloff who is charged with guarding a certain intersection in one of the cities, and it's very late at night and nothing is happening. He sees coming in the distance a funny kind of apparition. It seems to be a man walking. He has a top hat on his head. He is carrying in his right hand a candle and over his left hand he has a white sheet.

The apparition approaches Umloff and obviously senses that he is being queried. And the apparition says, Well, my name is Emil Kratzig. I died last night. This is a seventh class funeral.

Now, isn't it possible that we have allowed the system of disclosure to embroider itself into all kinds of senseless restrictions—each step of the way may have made sense at some time, but haven't we accumulated far too much?

In order that I not be recorded here as entirely destructive, I have two suggestions. They are fundamental I think, and one can always make fundamental observations if one doesn't know much about the subject; all observations are then fundamental, so that's why these two seem fundamental to me.

Can't we do some management by exception here? It's a well-known principle. Why isn't everything releasable except—and then let someone who is officially charged with so doing cite the exceptions?

Now I would observe that in the Department of Defense a Major—and I'll make up my rules as I don't know them—but someone like a Major may sign a contract for $50,000. It takes a Colonel to do half a million, and a General has to approve let's say $5 million. Don't hold me to the numbers, but we have that kind of hierarchy of approval. It naturally follows, of course, that the General is smarter than the Colonel and can approve the higher number.

Because failure to release equipment abroad has the reverse effect if you want to sell it but can't sell it although somebody wants to buy it, I think that Majors should withhold the sale of equipment that probably would not accumulate to more than half a million dollars. But I think if we're going to lose the sale of as much as $5 million, maybe we ought to have a Colonel or an equivalent level in the Department of State to withhold the sale and perhaps an Assistant Secretary of one department or another approve any action the consequence of which is to prevent the sale of that equipment abroad.

I say that at the risk of having the sales program measured entirely on the numbers involved. The sales program is not entirely, if indeed it is at all oriented on, the pure benefits to the United States. Military equipment unlike any other kind of equipment, first of all has to be eligible for sale. This involves a complex series of criteria, the best example of which is to ask how many F-4s shall we sell to Israel before we start to make the Arabian countries there excessively nervous. That's a classic problem that often gets to the President. It has nothing to do with disclosure. But in all those criteria the level to decide something is proportionate to the importance of the problem. I can decide some things of absolutely trivial importance. The President has to decide things having to do with Israel and the Arabs. It only goes to the White House after a great deal of consideration by all departments involved.

Clearly our whole Government is organized the same way. The level of importance should be proportionate to the level handling the matter. But I have the feeling that we have some people in our defense system at least who are making highly significant decisions with regard to the release of equipment for foreign sale who do not appreciate, are not knowledgeable about, if I may say so, couldn't care less about, the impact on all the things that come in train after you make a formal refusal to release.

So I would suggest that those of you who are laboring in this field, and especially if there is an Emil Kratzig among you, that you look at management by exception to see if we can't find a system that doesn't control everything but only controls that which should be controlled.

Mechanical engineers have known for 150 years that you don't have to watch the speed control on a steam engine to make it go faster or slower. You put a governor on it. Why can't we do the same thing here? Why can't we exploit some automatic actions?

The best automatic action I can think of is the self-serving instincts of a corporate board of directors. I think we ought to establish a system in which the basic criterion—I'm putting aside now things of national import like a nuclear capability or something like that; I frankly wouldn't know how to do it except to control all of it—but, let's have a threshold below which certain automatic things are allowed to happen. Let me make my point by analogy.

The world outside of the United States, the free world that buys military equipment from the United States, much of it is increasingly interested in producing more and more of that equipment for itself. This is called various things. We call it co-production when they want to produce it for themselves. A classic case: the Republic of China is now beginning to build F-5s. The question comes: should the United States approve China building the F-5?

Well, right away, you can understand, we really would prefer to build the F-5 in the United States and sell it to China. So the criterion becomes, what is the local content that's involved? We tend from a purely selfish point of view to favor low local content. That is to say we would rather have China, if it has to build part of the F-5, build only 10 percent of it instead of 50 percent of it—from a purely selfish point of view, putting everything else aside. I assume that there is a military requirement for it and the political relationship is such that we can do that.

It comes down now to the construction of the program. How shall we try to influence this?

Well, one man has suggested that we'd rather sell from the United States, especially in these days. The difficulty with that is if you try to legislate that kind of a position and veto any kind of local content in these sales, they'll buy French or buy British and you'll have 100 percent of nothing instead of, as in the Chinese case, 93 percent of something.

Now, this is an active debate right now. How shall we go about controlling this? There is a school of thought that says we must have a big committee—State, Defense,

White House, OMB, Commerce—a committee that will study all these criteria of balance of payments and local contents and licensing situations and the willingness of, in this case, Northrup to facilitate the co-production. And I'm suggesting that in that ongoing dialogue, you don't need a committee. Go to that organization concerning which I guarantee you will make precisely the right decision and that's the Northrup board of directors, because that board is not about to arrange for co-production abroad with local content 1 percent more than that required to make the transaction go.

Let them, let people who have a self-interest judge it, and I assure you that no Governmental committee can do any better.

That argument won, by the way, with regard to the Chinese case. And the 93 percent falls out of very intensive negotiations between that firm and the Republic of China.

Now, if Northrup could have established a similar program with only a 5 percent local content, I'm sure they would have. And I'm sure they would have gone to 15 if that had been the nature of the company's judgment about the likelihood of the country's taking on that program or adopting some other aircraft.

Let's exploit the built-in self-serving characteristics that are in our system. Let's try to quantify the value of something instead of making policy decisions about its releasability.

Let us do what is happening in another aspect of our Government. I'm not sure I want to talk about the specific case. But there was last year a major question that went to the White House with regard to the release of some very advanced technology to a European country. It was of national import. The answer was, No, we do not want to release it; the technology is too advanced; it is of such great value to the future of U.S. aerospace we don't want to run the risk of releasing it.

The question is coming up again. Now the answer is turning on, and I think it will come out this way, we won't say yes or no. We're going to say yes, but it's going to cost you a leg and an arm.

Let's put a value on that technology and if the buyer wants to buy it, then let's take the proceeds of the sale and put it back into U.S. R&D and maintain the supremacy we are trying to guard. The guy that can best sort out the values involved in this case, too, I think, is industry and not Government.

Somehow we're going to have to exploit this guaranteed operation which is as guaranteed as the governor on a steam engine. No corporate board is going to do anything except maximize the benefit to that firm. Use that enormous horsepower, instead of having functionaires sitting within Government trying to make routine decisions, the economic consequences of which are beyond them.

I lived in Paris for five years and I stayed out of trouble until the fourth year when I got a traffic ticket and I was invited down to the prefect's office. He was very courteous and he brought me in and sat me down, and brought out a file that was about an inch thick with Alne, Leonard A. in old Norman script on the side of it. And the thing was dog-eared. It looked like a working file they had used every day. And that's the first time I knew about it. I'm sure that my presence in Paris—I was a little functionaire myself in the U.S. Embassy—kept some other functionaire busy keeping track of me. And then I didn't even know it and nothing ever came of it. It was a purely wasted exercise.

If there are any Emil Kratzig's out there doing that kind of work in regard to disclosure I would invite you to rebel.

Questions and Discussion

Question: Mr. Alne, would you tell us what is your interface with ISA and the disclosure route for export license release?

Mr. Alne: Yes. Until a year and half ago this operation that I direct in sales was part of ISA and that portion of ISA having to do with trade disclosures, Dr. Mountain's office, was simply another adjacent office in ISA. As a matter of fact until 1965 the function of trade control was in the office that I'm now in. But it was decided, I think for good reasons, just as you don't have one man in your office handle both accounts receivable and petty cash, so you shouldn't have a man that handles sales also handle disclosures. He's obviously disposed to disclose. So we moved it down the hall.

Then a year and a half ago the Defense Security Assistance Agency became established and its Director reports to the Deputy Secretary of Defense. Technically there's no ISA within the range of vision of that Agency.

You can visualize it as the operating arm of Security Assistance. That includes grant aid, small in scope, and sales. We have three directors in the office—sales, grant aid, and the comptroller. But we are operationally oriented. We make no policy. I'm very happy to concede all kinds of veto capability all around the city with regard to sales. If I don't have them unanimously in favor of the sale I don't make the sale.

Question (Mr. Robinson): Mr. Alne, may I ask, in connection with the fact that DSAA is relatively new, I would suppose that it is examining policies that may impact in these areas and one might look forward to their examining some of these which have been brought up this morning as to the overall impact, or you will perhaps come to it.

Mr. Alne: It's not presumption. It's just wrong. There is a lay view even around the Pentagon just exactly what we should be doing. I get all kinds of questions like that.

As a matter of fact, what we're trying to do is get through the day without stumbling on major transactions. I'd love to say I directed all those $4 billion worth, but a lot of them took place routinely in the military departments. There's nothing pretentious about most of them. There were no major negotiations.

We concentrate on the other portion of the spectrum which I would describe as not directing anything, but orchestrating all of the influences on the master decision whether we are to sell something or not.

By that I mean that there is an expert for everything someplace in the Pentagon. None of them is in my office. They are all elsewhere. What I have to do is find out for example when the Kuwaitis, as they now do, want to buy a modern aircraft, want to buy from the United States. Then questions come, what is releasable to them, and that

comes out of the whole disclosure system. What is the price of it? What is availability? What is the impact on U.S. forces? What is the impact on U.S. planes on that production line? What configuration options are there? All of that needs to be in the service. Industry—my office I think probably has more relationships with industry than anybody else because I happen to be vigorously in favor of government-industry teams. I'm not winning all the time on that argument. I must say that military departments tend to be a little bit standoffish about that. They frankly don't like to have an industry member on their team today when they're selling an airplane to Kuwait and then turn around tomorrow and sit across the table and negotiate the price of the aircraft, in that sale.

But I believe that industry has to be part of it, that the best way to answer questions when you go out to Kuwait and you didn't anticipate exactly what was needed, is to have an industry member on the team if the equipment has been selected by the country and there is not some other U.S. competitor that you have to be arm's length from.

That's the most powerful way to operate. I want industry as soon as the Kuwaitis select an aircraft, I want that member right on the team right along with negotiations. If there are occasions when the other government is not comfortable with industry, I'll have them out in the hotel but they should be part of the team.

I was told one time that the Venezuelan government did not want this certain firm within five miles of the capitol during negotiations. So I said we'll put them in a hotel six miles out of town, because they're on the team.

You can't really sell an aircraft or a major system without industry. We don't have any such aircraft. We don't produce them. We wouldn't know the first thing about it if it weren't for the firm that is producing it.

But we're dealing in transactions. We're trans-actionally oriented. Because in defense there really isn't anybody else around to answer questions like how's the military sales program going; what do you think of the multilateral concern, the multinational corporation, and all these other basic questions that I don't have time for that I'm asked about indeed I'm tempted today to wonder if as so-called Director of Sales I shouldn't look into all the impediments that appear to be slowing down sales that I hear about this morning. But I frankly will probably get back to the Pentagon and get inundated by what's gone on since 10:00 o'clock this morning and I'll just get at it.

I must say in all seriousness that I'm discouraged by the deliberations today, because I really think we have gotten into some kind of an operation that moves forward by momentum, that picks up like a ratchet all new requirements without relinquishing the old, so that we're getting more and more convoluted and elaborate like a Steig drawing in the New Yorker, you know, all these things going around. I really feel that we are participating in a self-inflicted wound that must be corrected. But I don't quite know how to get my hands on it. One of the Emil Kratzigs out there is going to have to do it.

Question: What adverse effects have been noticed?

Mr Alne The sales of sophisticated equipment have been prevented witnout the planning of it. So it has had an adverse effect.

I think Conte Long I think it's falling out of current legislation because I think it's being recognized that an F-111 is obviously too sophisticated in some countries; but that a varnished bow and arrow may be too sophisticated also in some countries.

Someone mentioned the general atmosphere with regard to sales, and it is true. You think you've gone through some nonsense. We've gone through some too. We've had legislation and still have that we must not sell over a certain figure to Latin America. I think it's now being recognized that that's rather silly to limit the United States to $75 million to $100 million when England and France are selling $500-$600-$700 million. So Mr. Rogers announced about two months ago on the occasion of his trip to Latin America that we now recognize this was too paternalistic to somehow coerce Latin American countries into building schools by withholding from them the purchase of military equipment. I guess that's great if you can do it; but the fact is they then went off and bought from England and France; and so we recognize that maybe they are sovereign countries and maybe we ought to let them make their own decisions within limits. We don't have to participate in excessive sales. We don't have to look like we're encouraging arms races between countries. But it really is a bit much to say to Peru that it cannot get rid of a 20-year-old airplane which costs more to maintain than it would to buy a new one. And it's a bit much to tell a country it doesn't have an enemy and doesn't need any airplanes—I suppose that's true. But if a country wants to have airplanes if only to fly over the parade ground on national day, I suppose that they ought to be allowed to do that.

I'm not in favor of selling anything to anybody, but I am opposed to treating a region as we have done with our legislation. We don't sell to regions. We sell to countries. And Brazil does not like to be told it can't buy something today because Nicaragua bought something yesterday. That's just not within Brazil's range of interest. And for us to impose that on them in a regional way I think is condescending, it's paternalistic, it is aggravating, it is abrasive, it is not effective, and I think the Congress is not recognizing that.

On sophisticated weapons, the point of it is all right, but we were doing it all the time. We never did sell F-111s to Ivory Coast, for example, and we're not likely to.

As Mr. Florence said this morning, all of your disclosure decisions are really states of mind. They are judgments in the mind. Well, so are these judgments. Frankly there are many other criteria that outweigh the simple fact of sophistication. Sometimes sophistication so reduces the maintenance cost that a country should have solid state electronics instead of vacuum tubes. There's no law that says you should go through vacuum tubes before you get to solid state. What's important is what best fits your requirement. So sophistication, that criterion, really translates into what is manifestly excessive in quantity or value or in operating sophistication. It would have been treated under other terms as well.

Question: Are you able to deal directly at the outset I'm a representative of a foreign government or a foreign industry, and I want to come and buy something that belongs to you, that your industry is selling. Do I come to you after U.S. industry says, Gee, I can't sell it to you

direct? Do I come to you and get you to help me get that thing sold?

Mr. Alne: I suppose that could happen. The law provides that we are authorized to sell either from stock or from new procurement, so that its title passes temporarily through us and onward to the buyer.

Question: Strictly through FMS?

Mr. Alne: If it goes through Government, then it is FMS, right. But the law also provides, has provided for 20 years, that the Department of Defense should not participate gratuitously in the sale of equipment to foreign countries. That is, if it is generally available from industry, we shouldn't be in the business.

The fact is, as you've seen from my numbers, 75 to 80 percent of what we sell from this country does go through Government, so it brings us to the question, are we unfair competitors of U.S. industry?

Some can allege we are. It depends on the industry. Most do not. Basically, major systems are very hard for one firm to sell. McDonnell can't sell an F-4 because it doesn't produce the F-4. It produces about 25 percent of it. And the Government-furnished equipment that goes into the F-4 is very difficult for McDonnell to buy. If it does try to buy it, it would be a high cost procurement. So just by the sheer facts of the matter, countries often come to the U.S. Government to buy major systems.

I once calculated that when you go through the first 17 major systems you exhaust half of our military exports by value because of the skewing effect of the value of major systems.

Secondly, there is a trend that countries want to come and buy from the U.S. Government because with us they know that we will then buy on their behalf with the same prudence that we do for ourselves. In effect that means that some countries who deal a great deal with us, like Iran, stop just short of signing a blank check in their orders with us. Because if they sign a letter of offer they know that letter of offer says that the price is estimated but we're doing our best to estimate it accurately, that the delivery is estimated but we'll do our best to meet it; we're not giving you these numbers casually, a lot of work has gone into it; and now we'll go negotiate with the firm and buy it for you if you want us to do so with the same vigor that we do for ourselves. So they don't know exactly what it's going to cost. But they do know that they will not be taken by a firm who is disposed to do so. They are guaranteed equitable treatment by the Department of Defense. I think we've earned that reputation, frankly, and I know we have it in almost all countries that I can think of.

So DoD has an enormous advantage over industry because we're credited with not being profit motivated. By law we can make neither profit nor loss. So countries tend to come to us.

The law, by the way, that I mentioned speaks of developed countries We shouldn't sell to developed countries that which is generally available. The law says we can sell to less developed countries whatever we want. So even developed countries come to us and, frankly, put me in a dilemma. One man from Europe said to me one day, I understand your law, your regulation, about commercial availability; but if you don't sell to us we'll go commercial like you say? but what makes you think we'll go commercial in the U.S.? We'll go commercial in Europe. They're a lot closer. I don't prefer to deal there. We get better quality here on an average and your price—he said this two years ago—your price is not all that bad—now I think we would say it would be much better here because of devaluation. But we put them at a huge handicap to make them come and deal and search out and negotiate with you in industry. And some of the Middle Eastern countries have been inundated by salesmen from all over the world, from Europe and the United States. They really can't handle it.

We don't even pretend with Iran. Iran makes us formally and officially: We want to buy only from the U.S. Government. The Government agreed. It wasn't casual but it was a deliberate agreement for all the reaons of policy one can imagine between us and Iran. So we don't even go through the commercial availability syndrome with Iran. If they want to buy from the United States they can do it.

The difficulty, of course, is in the case of the other gentleman I mentioned, I don't want to cut out a U.S. firm that has developed a market and just short of selling have that market pulled out from under it. On the other hand, I do not want to be so formal and so literal about following that admonition of the law that we put business elsewhere. Business that wants to come here—all these concerns where it is valid for the United States to sell the product. We made a deliberate decision, not I, but in the Department of Defense some months ago that this country was in no economic condition to run that danger. So we tend to be a bit more relaxed. We get complaints, especially from the electronics industry, and they often write to their Congressmen and we have to answer them. We are trying our best to be equitable to all concerned but I'm not sure we always achieve that. But we did sell $4 billion worth.

Question (Mr. Florence): Would the industry representatives comment on whether any of your sales processing problems stem from security classifications being put on your company-owned information?

Mr. Fredericks: Very definitely. Information that we generate, our own technology, may not even come from the facility in which we're developing a weapons system or an electronics system is what I speak specifically of. Yet we ultimately find that being classified.

Question: I wonder if you could apply one of these little comments I heard just a moment ago, exercise your own self-serving interest, and not permit those classifications to be put on your own things.

Mr. Fredericks: We don't accept it without resistance, but sometimes we have no recourse because in the final analysis—and I think the comment was made previously today—our big customer continues to be the U.S. Government, the three military services; and ultimately our self-serving interest sometimes has to be served by recognizing who our big customer is.

I'd like to continue to go back to a point that was made. In our marketing activities internationally we are prepared and we do approach customers on the basis that we will negotiate a contract directly with them. Nevertheless we recognize that some of these same customers do have recourse to the services that Dave spoke of and make an FMS case out of it.

In the final analysis it's really immaterial to us as long as we do our homework properly, and there's a lot of promotional activity that we feel is necessary for us to do and we're not alone in the industry in that respect. Sometimes that's the way that a foreign military sale is actually started, from efforts on behalf of an individual company going out and making their capabilities known to somebody who has a requirement. Then they ultimately come back and ask the U.S. Government to produce it.

So this is the industry-government team that Dave speaks of in operation. Sometimes it has more visibility than at others. But it does continue to work.

Mr. Silver: Bill, did you want me to comment too?

Member (Mr. Florence): Please. Having had some experience with the very fine company you represent, I'd like also to have a comment from you.

Mr. Silver: I have a specific example I'll cite for you. Recently we went to the State Department with a brochure on a product called the ADT-19, which is a laser designator. It had been procured by the Army as an unclassified item, unclassified hardware. We had a DD 254 that told us it was. Part way through the procurement the Navy bought one of these. The brochure we sent to the State Department as an unclassified document identified that at one time the Navy had been interested and had conducted experiments with this device. That's all it said.

The brochure was returned to us by the State Department with a notation: This document has been determined to be classified. We recommend that you resolve the classification and after the classification has been resolved—something to the effect that there is every indication that you would be eligible to receive the export license you initially applied for.

There was no indication of what it was that made it classified, what the guidance was that we should be following, or what group category it was in. It was only through an intelligence effort on our part that we were able to determine that it was the Navy that had placed the classification on it to begin with or in the processing.

This case is presently in the State Department. I don't know what's going to happen. I responded by deleting all references to the Navy and resubmitting the document.

So you say is there something we can do. If you're going to get the document cleared, you're going to have to compromise someplace.

Mr. Fredericks: This is the double-bladed axe that the new initative program poses to industry. DoD and the several military services come to industry and say, you come to us and tell us what you have to offer that will meet a need that we have, and include in that the design-cost concept. We're not alone in having done this. Other people have done so. But in the process of doing so, using our own technology and at our own expense to get to that point, there are people who read into this things that may impinge upon what they are doing or have responsibility to see is done on an existing U.S. Government contract. And there the compromise has to be made.

And we don't always have all the flexibility and latitude you need in order to act conclusively in your own best interest.

Member (Mr. Florence): May I make one little comment with you, both of you, on the experience you are discussing.

I have in mind our new Executive Order that has come out all of a sudden with a representation that purports to say we're going to apply sanctions against individuals in the U.S. Government who put unnecessary classifications on information.

Now, at some point someone is going to get real strict on this and look around and see where else they can apply sanctions. And it could be that they would come along to these commercial firms and cause action by contractual clauses for the commercial firms to begin applying sanctions on unnecessary classifications.

This was just sort of in my mind in your operations I've heard described today.

Mr. Silver: I would answer that by saying that industry does what it's directed to do.

Question: I'm surprised to hear that governments would come to the Pentagon to buy something from them with all the horror stories I've read in the media about cost overruns. Do you get any requests for a C-5, for example?

Mr. Silver: They only want the successes. They don't ask much for the horror stories.

Member: I think if I were XYZ Company, I wouldn't want the Pentagon buying anything for me. I'd take my chances of negotiating with McDonnell-Douglas myself.

Mr. Fredericks: But you can't always assume that what you read in the newspaper is right and I think that that's the approach that they take. They have a show me attitude that they're willing to undertake.

Member: I might support the position that, if the foreign government buys through our military system from us, they also have the advantage of the in-house inspection of the hardware which is probably important in the airplane industry.

Mr. Aine: Yes, but they can get that commercially too. They have to pay for that in either event. Your point, sir, is applicable both to FMS and to commercial purchase, purchase through the commercial channel of that same horror. If one such horror exists and the buyer wants it, all I'm saying is if he has to buy it he may be suspicious of the price or he may read it in the papers also and have the same disposition that you do. But if he needs the equipment, all I'm saying is he tends to want to buy it through the Department of Defense because at least he knows that we will do our best to achieve the lowest price.

Question: Is it feasible or possible that a government would come to you to seek a product and you would say to them, we'll help you buy this product but you go direct to the industry?

Mr. Aine: Yes, we often do. I don't know what you mean by help but we often do refer them to known sources and we go through all the mating dance of advising because of the law and because there's no need for us to be in the business.

Question: I was thinking about arranging a loan.

Mr. Aine: Oh, indeed, the U.S. Government offers credit but that's another story we haven't gotten into yet. That's to less developed countries, highly limited, indeed non-existent if the current Congress has its way—sorry, if last year's Congress has its way, which it did, for an entire year. But we have something like, historically, half a billion dollars a year, not a grant fund but a credit fund, which is all repaid to the United States. ■

CLASSIFICATION AND THE SMALLER RESEARCH GROUPS

Mr. John D. Kettelle,
President KETRON and Vice President
Military Operations Research Society

Security in the Department of Defense recalls the first line of *A Tale of Two Cities,* where Dickens said, "It was the best of times; it was the worst of times." I think it is easy to say, "We have the worst possible security system; we have the best possible security system." I think that whatever I do say will be in a context that there are some horrible things but there are some good things; that somehow it adds that there may be some room for dramatic improvement, but I am not certain precisely where it is.

The situation is a little like the judge's son who was being admitted to the bench and who was told by his father, "Never give the reasons for your decisions; your decisions are probably going to be right but your reasons will almost certainly be wrong."

These remarks are from the point of view of a typical small company primarily working on classified study projects. What are some things of concern? Deciding how to classify documents, determining a need to know, and a lot of other details. Most of what I have to say will be on the classification problem. Now, actually, there is no classification problem because of the DD 254s, right? *Just follow what they say and you know what's classified and what isn't.*

As mentioned, I did study mathematics. Let me retreat into mathematics for just a few minutes. There is in mathematics, and also in a lot of military work, a classification problem which hasn't anything to do with security. Typically it's classifying targets—are they friendly or enemy, are they decoys or real targets? That sort of thing. Is there something there or not? That's a classification problem.

The classification problem may be discussed using the graph in figure 1. Let's say there are only two classifications, Unclassified and Secret. The horizontal axis is the fraction P(S/U) of documents you are going to classify as Secret, which are in fact Unclassified; and the vertical axis is the fraction P(S/S) of documents that are Secret that you are going in fact to classify Secret.

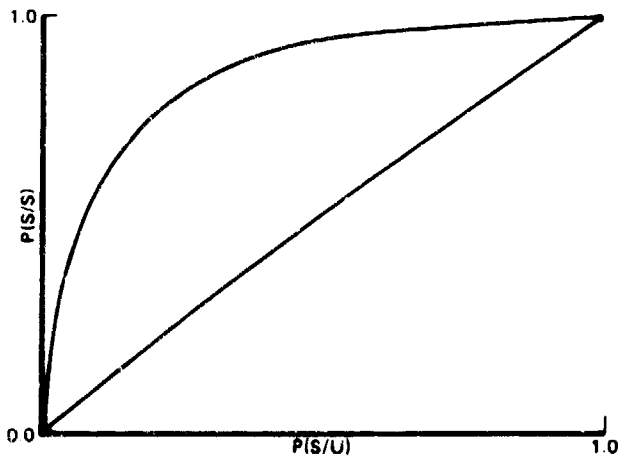


FIG. 1: OPERATING CHARACTERISTIC FOR CLASSIFIED DOCUMENTS

Given some intelligence that you have about how to classify things and the amount of time you want to spend worrying about it, you can operate anywhere on a certain curve, which is called an *operating characteristic.* There are two trivial points you can always attain. First, you can classify everything Secret, in which case the probability you classify Secret documents correctly is 1.0 and the probability you classify an Unclassified document is also 1.0. This is the upper right hand corner of figure 1.

On the other hand, you can refuse to classify anything Secret, in which case the probability of classifying Unclassified documents as Secret correctly is zero but the probability of classifying Secret documents is also zero. This is the lower left hand point of figure 1.

You can attain a 45-degree line, as in figure 1, as long as you don't try to get smart. A 45-degree line says if you want to make sure that half of your Secret documents are correctly classified, flip a coin for every document, and you'll be sure that the Secret ones have a 50 percent chance of being correctly classified, and so do the Unclassified ones.

If you have some misinformation about what somebody, you know, *The Source,* thinks should be Secret, you can do worse than that. You can fail to classify less than half of the real secrets and classify as Secret more than half of the trival or Unclassified information.

Generally speaking the kind of curve that you can attain is one that is above the 45-degree line. In the illustrative curve, if you are willing to accept misclassifying something like only 10 percent of the truly Unclassified information you can correctly classify something like 80 percent of the information that's really Secret.

One project where classification was really important was the Ballistic Missile Early Warning System. Our work was involved in the analysis of how much about a target do you have to learn in order to think it is a missile; and, how many missiles reported from various sites do you require in order to set response levels for SAC.

In those days, when we really thought that nuclear war might be right around the corner, some false targets almost generated an alarm. Fortunately, that was the day Khrushchev was in New York pounding the table with his shoe, and that helped our operating characteristic.

Now, in such projects there were some real secrets in the classified information sense. There was also a lot of mathematical analysis which the analysts wanted to publish. You kind of enjoy publishing and maybe it would have done the world some good. We never had quite enough energy or possibly time to sanitize the work so as to publish it. I think frankly most of the time we thought we knew what was really Secret and what wasn't. It's not too big a problem, in spite of the fact the DD 254 was thought of as primarily a formality you had to have when the security inspector came around.

I think there is an interesting theoretical problem that relates to this. It's what I would call a *Catch 22* effect: the *rule* about what is Secret and what isn't may be more highly classified than Secret.

An example which is no longer classified comes from World War II. In World War II, there was a high frequency direction finder system, commonly known as HFDF. German submarine admirals were very nervous and liked to have their submarines report in once a day. As a result,

our long-range radio direction finders were able to track the German submarines quite well, even if they didn't give their hull numbers. It was a fantastically important piece of information and probably changed the course of the submarine war in the Atlantic very significantly.

Somehow this reminds me of my Civil War History teacher at Harvard. He had ten separate lectures on what won the Civil War for the North. That wasn't as bad, however, as my Sociology professor whose final exam was: describe the universe and give two examples.

To return: there we were receiving all the information about HFDF, an extremely sensitive program at the time. Now, if the defense community and its contractors had been told that any mention of HFDF was Secret and shouldn't be included in any document, obviously that in itself likely would have been more highly classified than the routinely reported information—a situation similar to a number found today.

To avoid publishing the rule, theoretically, you can say, "All right, fine, let's hire 10,000 security inspectors. They won't tell you the rules but they will read everything you write and cross out the information that is highly classified." Even then you can imagine that an intelligent contractor or a civil servant observing what gets censored could "zero in" on what the rule was; so it really is a *Catch 22*. I think a certain amount of sloppiness in classification probably is unavoidable and may be desirable.

To proceed—how then *does* a small firm address the classification issue? Well, there's nothing magic about it. Nine times out of ten you know more than the project officer, assuming there is one. So you don't want to bother him—you just follow your own knowledge. The one time out of ten when he knows more than you, you probably don't want to admit it. But seriously, in 15 years perhaps I have had one occasion, to discuss with a project officer what his view was on what was classified and what wasn't.

I think there is an important additional dimension relating to classification. I worked at Arthur D. Little, Inc. for five years. Most of the clients there were commercial, and there weren't security officers in the military sense. But, security was tighter in many ways than the Defense Department. If you are going to determine for a drug company what's the best way to peddle something, you obviously are not supposed to tell any other drug company or publish anything about it. It's pretty tight security, for proprietary reasons.

It really shouldn't be that way within the Defense Department, but it is. In other words, many times you may have a Defense client where, even though its project or information is not classified, there is a proprietary like approach. I think anybody, whether they are in-house or out-house, should be aware of that circumstance and should be willing to understand and abide by the fact that it is unclassified but proprietary—limited in availability. In contradistinction, you can have something which is Secret but can generally be shared quite widely within the cleared part of the Defense Department community. Many examples exist of things classified for proprietary like reasons, and that is a poor use of classification. But we can't reform the world.

It would be an awfully good thing for a company or an organization of DoD—either large or small—when they do put out a report that has unclassified analytical work as well as classified information, to put out a little guide prepared by the author (or somebody collaborating with the author) about how this report could be sanitized—either by expurgating certain things or by paraphrasing. Even a given classified paragraph commonly can become unclassified by deletion of a specific or two.

We might cover briefly the determination of need-to-know. It is theoretically part of the same problem. If an item is classified, what you are really saying is tell only certain people about it. Who you tell is part of the same ball of wax. How to determine that, I think, is an area where there is room for a great deal of what I would call creativity.

I'll give you two examples. One is the library of the Center for Naval Analyses (CNA). The other is the Military Operations Research Society, of which I am a Vice President.

The CNA library you cannot get into without having a fight—you have to be cleared Secret if you are going to get into the Secret file, Top Secret if you are going to get in there. And, on top of that, CNA and its monitor, because CNA itself is sort of proprietary, will fight pretty hard not to let you in in the first place. But if you do get in, you have access to a much broader range of information than any cautious contracting officer would ever permit you to get at.

The same thing is true of the Military Operations Research Society. As you know, there are a lot of other "Secret societies." They meet once or twice a year. The Military Operations Research Society is probably a classic example. It meets twice a year and has maybe 600 to 800 attendees. It covers almost the entire spectrum of defense analysis; anything from undersea warfare, to urban warfare, to what have you. (Try to think of a way to use submarines in urban warfare.) Once you get your contracting officer to recognize your need-to-know so that you can attend, you can shop around and sit in on the tactical nuclear warfare problems associated with the defense of NATO or any other topic; a much broader access than usually associated with need-to-know certifications.

Now, I feel that all that is a very enlightened and good thing. It is close enough to breaking rules that people are very careful about it, on top of just being patriotically careful. It does give people a chance to find out what really is going on in a broad context to make them productive, rather than the limited perspective of things that apply only to a given contract. The search for solutions to problems requires freedom from the ordinary fences if an effective solution is to be found.

Now, let me go down the list of some of the typical mundane issues that a small company—and of course a large one—has to face.

The first one is you've got to write a security manual. I think that somebody has somehow designed the system so that you'll be forced to write one even though there is a sort of standard one you can practically duplicate. Theoretically that's supposed to be good for you; it makes you read it if you are going to write it. But I think that is a little ridiculous.

There is no question in my mind it would be a good thing if there were a couple of firms or individuals who were available to small businesses, to help them set up

their security system and give them somebody to talk to in confidence (just as you would to a lawyer), about their security problems. In my view the security inspectors are really a very friendly, understanding lot, but you don't know that at first and, understandably, you cannot consider them a confidant. Such a firm could start off by working up a security manual for you, and sort of "hold your hand" during the first inspection or two.

In my view, security inspectors are not really out to try to hang anybody. They are out to make sure that things work reasonably well, and if somebody is really out of line they will naturally have to get involved. But they are not just waiting for somebody to make a mistake.

There is a phenomenon, I believe irrefutable, that the further you get from the Government, the more nervous you get. Consider an organization or company large enough to have a security officer. The company security officer may also be fairly benign, but by the time we get around to some divisional security officer we are likely to find him three times as strict as the Government is. Now some of that "over-security" is a good idea, but I think that you can generate a lot of hate and discontent in a company by being a little too picayune.

Another important item is the return of documents after a project is completed. That is usually the main problem we have after the security inspector leaves us, other than cheering up the secretary who is our security officer. Parenthetically, the small company always has a secretary as security officer. That, by the way, is a very good idea. She's usually a lot smarter in these matters than any of the analysts and takes it very seriously. She'll come in and she'll say, "Well, we have this report that we've had for two years; the contract expired a year ago, and the inspector says we've got to return it to the contracting officer."

In my view that is a problem. I realize that a lot of people would like to "squirrel" reports, and you have to have some way of making sure that you don't get too much hoarding. Nevertheless, it's a tough problem for us. A big company often has other contracts, and usually can relate these so that the documents are transferred to another contract.

This gets back again to the CNA library. If you are going to propose a study, often the RFP and people that issue it will arrange for you to have access to some documents, in order that you can write intelligent proposals. So it is *possible* for the Government to organize little ad hoc libraries.

I think this is something the Government ought to do more, so that the contractor who feels that he has certain strengths and maybe a little bit of experience in an area, with the proper permission would have some way to have access to the literature in that area. That would make me a lot less nervous about having to destroy my own documents. For example, if I knew they were going to be shipped to a place where I could immediately refer to them on appropriate occasions, I would feel more secure, and less concerned about their retention. These are a few of the aspects that seem to impact especially on the smaller research organization. ■