

6

CLASSIFICATION MANAGEMENT

Journal. Volume X - 1974. Papers from
The National Seminar (10th), 16-17-18 July 1974.

11 1974

12 110p.

DISTRIBUTION STATEMENT A

Approved for public release
Distribution Unlimited

JOURNAL OF THE NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME X - 1974

406 616 06 13:014

Published semiannually. Mailing address: Executive Secretary, National Classification Management Society, P. O. Box 7453, Alexandria, Virginia 22307. Lorimer F. McConnell, Editor. Views expressed by individuals herein do not necessarily represent views of their employers nor of the National Classification Management Society.

Copyright © 1975 by the National Classification Management Society

DEDICATION & SPECIAL RECOGNITION

The Board of Directors and the Seminar Committee dedicated the Tenth National Seminar to James G. Marsh and Daniel F. Rankin whom we all knew and loved.

The Society recognizes with regret the retirements of C. Donald Garrett, George McClain and Willard Thompson who have actively participated in NCMS for many years. Their unselfish contributions to the professional development of Classification Management is an inspiration to all those who follow.

| | |
|-----------------------|----------|
| ADMISSION NO. | |
| DATE | 10/10/66 |
| BY | |
| <i>Letter on file</i> | |
| A | |

CONTENTS

PAPERS FROM THE TENTH NATIONAL SEMINAR

(July 16, 17, 18, 1974)

>
Partial contents

REVIEW OF PAST YEAR
 Fredrick J. Daigle, President 7

KEYNOTE ADDRESS
 Joseph J. Liebling 9

THE GOVERNMENT'S SECURITY CLASSIFICATION AND DECLASSIFICATION PROGRAM
 William L. Brown 13

DOD PANEL: PROGRESS AND EFFECTS OF IMPLEMENTATION OF EXECUTIVE ORDER 11652
 Arthur Van Cook, Moderator 20
 Charles T. Grimes 25
 Frank Larsen 26
 Lawrence Myers 27

PANEL: LIBRARY COUNCIL LOOKS AT MAINTENANCE OF ESSENTIAL CLASSIFIED
 TECHNICAL INFORMATION
 Joe Ann Clifton, Moderator 35
 H. W. Jones 36
 B. W. Campbell 38
 John Berry 40
 Harold G. Hock 42
 Myer B. Kahn 44

PANEL: INTERNATIONAL SECURITY
 A. A. Correia, Moderator
 E. M. Silver 52
 E. T. Brown 55
 Rae Nehls 58

A LOOK AT THE ARMED SERVICE PROCUREMENT REGULATION
 Edgar C. Chapman, Jr. 63

TRENDS ^{and} DEVELOPMENTS IN INDUSTRIAL SECURITY
 R. E. Green 68

NEW-INFORMATION SECURITY MANAGEMENT COURSE
 John R. O'Leary 71

INDUSTRY VIEW OF INFORMATION SECURITY MANAGEMENT COURSE
 Fredrick J. Daigle 73

GOVERNMENT VIEW OF INFORMATION SECURITY MANAGEMENT COURSE
 Frank Larsen 74

EVALUATION OF INFORMATION SECURITY MANAGEMENT COURSE
 John R. O'Leary 75

PANEL: USER AGENCY PRESENTATIONS ON CLASSIFICATION MANAGEMENT FUNCTIONS
 Eugene Klein, Moderator 76
 Murray Marker 77
 Donald P. Ciesmer 80
 Joseph C. 82

CONTENTS (CONT.)

PANEL: PROTECTION OF COMPANY PROPRIETARY INFORMATION, *and*

| | |
|---------------------------------------|----|
| W. Pete Dennison, Moderator | 84 |
| Richard J. Healy | 84 |
| Richard A. Bardin | 88 |
| Lorimer F. McConnell | 90 |

CLASSIFICATION MANAGEMENT--DIRECT OR INDIRECT COSTS

| | |
|----------------------------|-----|
| John D. Tippit | 98 |
| Robert E. Bonson | 100 |

REVIEW OF LAST YEAR

BY

FREDRICK J. DAIGLE, President

On July 19, 1973, the present Board of Directors assumed office and the conduct of the Society's business. Officers are: Jim Buckland, Martin Marietta, Orlando, Florida, Vice President and Membership Chairman; Dean Richardson, Texas Instruments, Dallas, Texas, Secretary; and Sheila Dotson, Naval Weapons Center, China Lake, Treasurer. Members of the Board are: Jim Bagley, NRL, Washington, D. C., and Tom O'Brien, now Director, Security Plans and Policies, ODASD (Security Policy) Education and Standards Committee; Jack A. Robinson, Center for Naval Analysis, Arlington, Virginia, Editor NCMS Bulletin; Eugene Suto, Research General Corp., McLean, Virginia; Communication & Congressional Liaison; and, Jim Marsh, Sandia Laboratories, Albuquerque, New Mexico, who as past President, past Secretary, and coordinator for the editing and printing of the NCMS Bulletin, served the Society with every strength of his being, departed from our physical presence in December of last year. We all sincerely miss his wit, his keen insight and his deep devotion to the Society that he loved so well. In addition to the Board members, as elected, the following also served the Society with distinction this year: Mr. Donald Woodbridge, RMS Fusion Inc., Ann Arbor, Mich, our distinguished Society Counselor; Mr. Lorimer McConnell of System Development Corporation, Santa Monica, Calif. as our Journal Editor. In addition we have had the privilege to call upon our legal committee, C. Donald Garrett, George MacClain and Frank May, all retired and all in the Washington/Virginia area, plus Mr. Bill Florence who has been Special Assistant to the President for Congressional Information and has been responsible for the congressional mailings that you have received.

With this impressive array of talent we proceed on to what I think was, in many ways a successful year:

We first set objectives and they are as follows, with the results when there were any:

1. Prepare a follow-up letter to OSD on a previously submitted position paper on the subject of greater leniency in contractor retention of information on contract completion.

RESULTS: We received an indepth response from OSD on this subject indicating that they believed that the ISR and EO 11652 emphasized the "need to know" aspect and that the

responsibility for retention should continue to rest with the contracting officer and did not see a need to mitigate this responsibility by OSD intervention with any other system of handling retention.

2. Submit two additional position papers to OSD.

- a. We recommended the abolition of the LSM and incorporation of all requirements into one directive to permit the inspector and the inspected to both be working to the same set of requirements. In addition to the cost savings that would be evident by the need to issue and maintain only one manual. Also suggested coding the paragraphs numerically to the Information Security Program Regulation 5200.1R so we could better correlate and understand the dual standards when they exist.

RESULTS: OSD responded that this concept had been previously studied and was rejected and that the basis of rejection were still valid. Also that the ISR was policies, practices and procedures, while the LSM contained detailed security requirements, and the ISR was not intended to be applicable to industry, although they are available for distribution, and industry should not be burdened with maintaining them.

- b. We submitted a second paper recommending the establishment of a central repository for all classification guidance that is published, and recommended that DDC be considered as this repository, where any activity could have access to the multiple guidance on any one subject if in their registered field of interest.

RESULTS: This recommendation is still under consideration by OSD.

3. OBJECTIVE: Restructure the seminar to conduct the business meeting in a more efficient manner.

RESULTS: We snuck it in on you this morning.

4. OBJECTIVE: Support a mid-year mini-seminar in an area not normally supported by the annual seminar or chapter activities.

RESULTS: The Board of Directors participated in a supported one day seminar in Dallas, Texas hosted by Texas Instruments and Dean Richardson. Thirty to forty attendees from

the Southwest attended and classification management is much more meaningful to that group.

ASIDE: The Board earnestly solicits the opportunity to support a seminar for you in your area, or your command, primarily in February of each year, in conjunction with our mid-year Board meeting. We are available as speakers, panelists or just audience participants. If you are interested, please contact one of us. We are presently uncommitted for 1975. In 1973 we were in Orlando with Martin Marietta and this year in Dallas, with Texas Instruments. We don't charge and we do love to talk on our favorite subject--Classification Management.

OBJECTIVE: Update the Agency/Classification responsible person listing that we published several years ago.

RESULTS: The first draft has been completed and is currently being updated and will soon be published as an attachment to an edition of the Bulletin.

ADDITIONAL ACCOMPLISHMENTS have been the revision and redesign of the membership application blank and a rewrite of the NCMS Brochure, both the result of blood sweat and tears of our Vice President Jim Buckland.

And the last but what I believe the most significant, a complete revamp of the Society bylaws, bringing them up to date after ten years of practical application. All changes were administrative in nature and served to have the bylaws reflect the actual operation of the Society, all changes were within the authority of the Board of Directors except for the abolition of the Associate membership category, and making all members regular members. This was put to the vote of the membership by putting a ballot in the Bulletin, however only 60 ballots were returned; this necessitated sending personal letters to those who did not respond. This then resulted in a return of 116 votes, 115 for and 1 against the resolution. As this then represented a majority of the membership, the Board declared the resolution passed. As with any such task accomplished by committee, there were many suggested changes and attempts at the ultimate in the revision over a period of a year, until such time as we reached a selection of terminology that was acceptable to the entire board. Our most heartfelt appreciation for shouldering the complete burden of these rewrites, for his patience with those of us who

knew what we wanted to say but were inept with words goes to our Counselor, Donald Woodbridge. Thank you Don for a complicated task well done.

As a result of the interface by Director Gene Suto, the Society is now registered with the National Referral Center, Science and Technology Division, Library of Congress as a registered Information Source.

In October the Board approved limited support for chapters in financing the hosting of guest speakers in order to assist them in strengthening their programs and increasing their appeal to the membership.

In May, the Society was invited to participate in the Information Security Management Pilot course at the Defense Industrial Security Institute, Richmond, Virginia, and as I indicated earlier, the results of attending the course will be discussed in detail tomorrow by the school and by both the Industrial and the Government attendees.

In June, the Society acted upon the recommendations of the Nomination Committee headed by Dick Boberg of Sierra Research Inc., Santa Monica, Calif., also a past President, and voted on the slate of directors for the next three years and the selection of directors to fill the vacancies caused by death and resignations over the past year. Your ballots created a first in the history of the Society in that there were only 4 votes separating the first four successful candidates. Society policy is such that we do not announce the numbers of votes, however the ballots are on file with the Executive Secretary in Alexandria, Va. for audit should such ever be the desire of any of the membership. Elected for three full years were Dean Richardson, Jack Robinson and Gene Suto, all of whom were running for reelection. Elected for a 2 year term was Jim Buckland, also running for reelection. Two new electees are Richard Butala of Hughes Aircraft Corp., Culver City (So. Calif. Chapter), and Jim Manages, Applied Technology Inc., Sunnyvale, Calif. (No. Calif. Chapter Chairman), each for one year terms. So we have basically the same Board of Directors for next year, with two freshmen from whom we expect some new life and vitality.

The past year has seen all of us, both Government and Industry, going through the experience of a sparse budget, seemingly coupled with a pronounced increase in the responsibility and workload of the Classification Profession. Many of us were unable to travel as we had

projected, but in spite of this I feel that the Society prospered and progressed, and as all presidents before me, I know that I was unable to assist the Board in accomplishing all that we would have liked to as the calendar became an enemy rather than an ally. For your outstanding assistance, understanding and support I thank you all.

KEYNOTE ADDRESS

BY

JOSEPH J. LIEBLING

Deputy Assistant Secretary of Defense

(Security Policy)

Office of Assistant Secretary of Defense

(Comptroller)

It is always a pleasure for me to appear before the membership of the National Classification Management Society--a membership comprised of professionals who are knowledgeable in all aspects of the Information Security Program. I have learned, during my years in this field, of the importance of the free exchange of ideas through forums such as this and the benefits which are derived from such exchange by both we in Defense and you in industry.

I note from the agenda of this Tenth National Seminar that the presentations to be made in the time ahead will cover some very important aspects of the Program. I encourage your full and frank participation in the topics to be presented particularly, during the times allocated for floor questions and panel discussions.

We have just passed the second anniversary of the effective date of Executive Order 11652. It is appropriate at this time for us to reflect on our progress and discuss plans for furtherance of Program objectives.

During the past few weeks we have reported on our management of the Program to both the House and the Senate. In this connection, I should note that much of our progress in establishing the significant changes brought about by Executive Order 11652 and fully implementing its provisions is, in part, due to the continuing interest of committees in the House and Senate in exercising their oversight responsibilities.

The details of progress achieved by the Department of Defense will be discussed by Mr. VanCook who, for the past year, as my Director of Information Security, has contributed materially to the results we have thus far obtained. I would like to touch on some of the highlights, bring you up to date on legislation pending before the

Congress, and familiarize you with the views of the Department of Defense reflected in our reports and testimony with respect to legislation.

As you know, the Department of Defense Information Security Program is the largest in scope of any other Department of the Executive Branch with some 12,000 contractors and over 1100 major DoD activities involving several million cleared people. Our Program and the policies associated with its implementation are far-reaching. There is no doubt that the Department of Defense creates more classified information and material than all other Departments and Agencies of the Executive Branch combined. This great volume of classified material derives from the mission of the Department, the worldwide disposition of its elements and the sensitivity of its national and international operations.

The Congress has, by introduction of many bills in both Houses, indicated a deep concern that information about Defense policies, practices, and operations be given the widest possible dissemination, subject only to the restraints imposed by national security. We, in the Department of Defense, share that concern.

The overwhelming majority of the Department's official records are unclassified. These are accessible to the public, unless they are withheld for reasons other than security classification specified in the Freedom of Information Act. The public is now provided with a wealth of information on such things as laser technology, sophisticated communications systems and earth resources satellites which, a few years back, would not have been released due to its sensitivity. There has been a definite shifting of emphasis to further assure that the public is made fully cognizant of Defense activities. There is a wide range of media being fully utilized for informing the public such as daily press briefings and releases, publication of articles by Defense and industry authors in technical and scientific journals and wide dissemination of scientific and technical papers in the national and international communities. Other means of keeping the public and the Congress informed include our participation in symposiums and seminars such as this; appearances before Congressional committees and public speeches by Defense officials. In this regard, the Department has an excellent track record. To improve it, we are continually striving to reduce classification in the first instance, eliminate overclassification and accelerate downgrading and declassification.

In the past, the system of security classification allowed too many papers to be classified for too long a time. To deal with this problem, a comprehensive study was initiated by the President in January 1971 with a view to achieving a better balance between the two competing principles of releasing information to the public and of preserving confidentiality. I was personally involved in the early stages of this study which culminated in the issuance of Executive Order 11652. The Order established within the Executive Branch, a new and progressive system for the classification and declassification of official information relating to the national security.

By this time, the provisions of the Order and Department of Defense implementing issuances are well known to this audience. Consequently, I will not review their specifics. Rather, I would like to describe some of the more significant actions which have been taken to make the Information Security Program more effective.

Monitoring of the program is under the direction of Departmental Classification Review Committees, one at the Office of the Secretary of Defense level and one in each military department; a Defense Information Security Advisory Board; and inspection teams in the Office of the Secretary of Defense and the military departments. These Committees act on suggestions and complaints involving the administration of the Order and review appeals of requests for official records when a proposed denial is based on their continued classification under the Order. They are chaired by senior officials in the Office of the Secretary of Defense and in each Department who, in addition to their committee responsibilities, have responsibility for compliance with and implementation of the Order.

In addition to the departmental review committees, the Defense Information Security Advisory Board was established to advise and assist my boss, Secretary McClary, in the fulfillment of his management and monitorship responsibilities. The Board is chaired by me and is comprised of representatives from major components of the Department of Defense. With respect to suggestions and complaints, the Board acts as a working arm of the Defense Departmental Review Committee. The mission of the Board is to review and evaluate the effectiveness of the administration of the Information Security Program and to develop and recommend new or revised uniform policies, procedures, standards and criteria necessary to meet changing conditions, or to correct deficiencies in the Program which come to its attention. The

Board has considered and acted upon significant information security matters such as (1) improved security education and training programs, (2) the development and adoption of inspection procedures, (3) the gathering, maintaining and reporting of statistical data, and (4) the initiation of Program, Project or System declassification programs.

Within my office, a Division is assigned responsibility to monitor the Information Security Program through inspection and reporting. Since its establishment, its members have conducted on site, in-depth reviews of the Information Security Program at major Department of Defense component headquarters and at selected major Defense contractor facilities throughout the United States.

These surveys have helped the Department to identify strengths and weaknesses in program implementation and to effect improvements in the program.

To insure that the provisions of Executive Order 11652 are being carried out effectively at the working level, we have required Department of Defense components to report the results of their inspections. These show that during the period June 1, 1972 through December 31, 1973, over 2500 formal inspections were conducted within the Department of Defense components. In addition, approximately 10,000 informal reviews and security assistance visits were conducted for the purpose of making the Information Security Program more effective.

Among the more significant management actions are these:

First, in its continuing efforts to control the number of classification actions, the Department of Defense has consistently emphasized the need to reduce the number of persons who may classify information. Since the issuance of Executive Order 11652, the Department has reduced that number from 31,048 to 7,033 - a 77% reduction.

Second, the Department has directed continuing attention to limiting the use of the authority provided in Executive Order 11652 to exempt information from the General Declassification Schedule. We have ordered a detailed survey as to the extent to which exemption authority is used. We have found lingering tendencies to avoid application of automatic downgrading and declassification. This is one of the problems we are continuing to address. In this connection, I continue to encourage your challenges in those cases when you find security classification guidance insufficient or overbearing.

Third, we are reviewing security classification guidance for the purposes of accelerating downgrading and declassification where possible and restricting the use of exemption authority. We are paying particular attention to the declassification of total programs. The downgrading or total declassification of programs, projects, and systems or portions thereof has already resulted in the downgrading or declassification of tens of thousands of related documents. Many of you have participated in these actions and I encourage you to continue to carry out your oversight roles with the vigor you have shown in the past and make every effort to see that guidance in your hands meets current operational requirements. This is an opportune time to recommend declassification of programs which you believe no longer warrant security classification protection.

Fourth, the Assistant Secretary of Defense for Public Affairs has been authorized to declassify information originated within the Department of Defense. This delegation of declassification authority facilitates the review and declassification of testimony of Defense witnesses before Congressional Committees.

Fifth, we have issued guidelines whose effect is to declassify the majority of the Department's official records dated prior to June 30, 1950. To provide some indication of the results achieved through the use of these guidelines, the military departments have reported the declassification of 110,000 linear feet of classified records. The Archivist of the United States, who has been authorized by the Secretary of Defense to apply these guidelines to Defense records in his custody, has reported the declassification of approximately 50 million pages. These guidelines have also been authorized for use in such activities as the Hoover Institute, the MacArthur Library and the Library of Congress, all of which hold certain Department of Defense historical records in their custody. I might add that a study is currently under way to determine whether it is feasible to apply similar guidelines for the declassification of official departmental records as they become 20 years old.

Sixth, the Department undertook a project to reduce to the absolute minimum, consistent with operational requirements and national security, the number of Top Secret documents retained in files and storage. 180,469 documents were eliminated from the Top Secret inventory during the period February 1, 1973 through March 31, 1973 leaving a total of 541,539. We have plans to conduct a similar project during this calendar year.

Defense industry likewise has reduced its classified holdings from 15.4 million classified documents to 13.8 million. The result is that material remaining in inventory is better protected and costs associated with safeguarding are avoided.

Seventh, we have established an Information Security Management Course in the Department of Defense. This two-week course is available for both government and defense contractor security management personnel on a limited basis. Its purpose is to provide these personnel a comprehensive understanding in interpretation of all aspects of the Department's Information Security Program with particular emphasis on classification responsibilities. They, in turn, will be expected to pass on the knowledge gained through this formal training to personnel within their respective activities who are involved in classification matters. Additionally, through all available channels of information, the Department has stressed to its people that each has a particular responsibility to understand the objectives of the new Information Security Program and to do their utmost as individuals to achieve them.

As of March 31, 1974, the Department has, under the provisions of Executive Order 11652, received 582 requests from sources outside the Department for the review of 10 year old classified material for declassification and release. Of these, 534 have been acted upon and the information sought has been declassified and provided in whole or in part in 85% of the cases processed. In only 10% of the cases, have the requests for declassification been denied.

I would like now to turn to the proposed legislation which is pending before the Congress.

Underlying the proposed Congressional bills seems to be the belief that the Executive Branch has used the classification system to withhold or at least inhibit the flow of information to the Congress. Let me assure you that the Department of defense recognizes the concern of the Congress that it have access to classified information in order to fulfill its responsibilities. To this end, the Department has established policy that the Department of Defense components will make maximum information available promptly to, and cooperate fully with, Congressional committees, and that classified information not available to the public will be made available to the Congress in confidence.

The Department does have reservations as to whether the provisions of the legislation proposed will actually improve the operations of the present system. Many of the bills propose the establishment of a commission or a committee outside the Executive Branch with authority to control the classification and declassification of documents. With respect to this provision, the Department does not feel that it is the long term answer to dealing with a great volume of classification and declassification decisions which would daily face such commissions or committees. We believe that the broad powers of decision which are proposed to be vested in these committees or commissions would pre-empt the President's authority to classify information in the interests of national security and to restrict its dissemination. His constitutional authority in these respects is recognized in various statutes and by the Courts. The fact that the President would appoint the committee or commission members by and with the consent of the Senate does not neutralize the effect of the preemption. Such legislation would create a policy making body outside the Executive Branch with ultimate authority for classification and declassification policy determinations relative to information concerning national defense. The net effect would be that Congress would be determining what national defense information could be released to the public. The Department of Defense would, therefore, be limited severely in making determinations on classification, declassification and safeguarding matters of vital national security interest over which the Secretary of Defense must bear ultimate responsibility.

The vesting of this authority in a commission or a committee that does not have day-to-day exposure to the many factors and circumstances that control classification and declassification determinations would reduce the possibilities of achieving and maintaining a viable and progressive program. The decision to classify or declassify must of necessity be made by individuals who are ultimately familiar with and responsible for the substantive information under consideration. No external commission or committee or the staff of such commissions or committees, faced with the volume of decision making, could become knowledgeable of the many activities and programs of the Executive Branch requiring protection in the interest of national security to make sound judgments. Knowledge of complementary information within these programs is particularly critical to any declassification judgment. From what I have thus far discussed on the proposed legislation, I would not like to leave the impression that we challenge Congress's right to legislate to provide a statutory base for the classification

system. Nor do we challenge the Congress oversight responsibility in connection with the classification system. On the contrary, we encourage the continuing interest of Congressional Committees but in an oversight rather than a management capacity.

To go on, most of the bills currently pending provide for automatic downgrading and declassification at one year intervals. From our experience, we believe that the twelve month interval for downgrading and declassification is totally unrealistic. This time interval would fail to provide adequate protection for that information properly classified in the interests of national security. The Department's experience over the past two decades with classification matters shows that information properly classified would not lose its sensitivity to an extent which would permit uncontrolled dissemination in the proposed designated time frame. In all likelihood, original classifiers might tend to overclassify information in an effort to protect it for longer periods of time, thereby abusing the system and materially increasing classified inventories, and the storage, handling and transmission costs associated with the higher level classification. The bills which provide for automatic downgrading and declassification also recognize the sensitivity and need for extension of classification of certain information and establish elaborate procedures for accomplishing this.

We believe that the proposed procedures for referring to a commission or committee each request for extension of classification are administratively unworkable. For example, as I mentioned earlier, the Department of Defense Top Secret inventory as of March 1973 was 541,539 documents. We would estimate that the vast majority of these would require classification beyond the time limit permitted by the proposed legislation. Many of the requests for extension of classification submitted to the Commission or a Committee will involve information covered by statute, such as the Atomic Energy Act and other information concerning intelligence sources and methods, communications and electronic intelligence and cryptographic information. Such information has indefinite classification life and any declassification determination should be made by personnel who, as a result of day-to-day operations, have complete familiarity with the subject and are, therefore, able to determine the impact of declassification of the subject matter on national security. Consequently, these documents would require a minimum of three or possibly four

reviews by the Commission or Committee for extension of the classifications in highly sensitive areas. It is difficult to perceive how procedures could be established wherein this volume could be processed in an orderly manner and yet, still be responsive to current operational requirements.

Executive Order 11652 expressly recognized that "The interest of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public." At the same time, it acknowledged that "There is some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our nation and the safety of our people and our allies." The Department of Defense, like all other departments and agencies in the Executive Branch, has made progress toward achieving these complementary goals. We expect and will achieve further improvements in the Department's information security system.

Of necessity, the progress has been evolutionary. Certainly, it may be slower than some of our critics would like but nevertheless, it is effective. It is indeed difficult to articulate black and white solutions in implementing a program of this great magnitude and complexity within available resources. We have introduced a new system to the millions of people in Defense and industry worldwide. The re-education process is an undertaking which cannot be accomplished overnight. We are dealing with a system which depends ultimately on the exercise of sound individual judgment.

In the days ahead we will be working together toward achieving the overriding objective--responsiveness to the needs and interests of the public while safeguarding sensitive information. We are reviewing all proposals of significant interest which are made available to us and which are designed to meet this goal. I encourage your input. I believe that the facts which I have laid out before you and the additional ones to be supplied by Mr. VanCook this afternoon fully support the statement that since Executive Order 11652 was promulgated, there has been a vast improvement in the system.

Philosophically speaking, in a democracy, there is no security in unnecessary government secrecy. We are on course with reasonable management techniques to make the Department of Defense Information Security Program a most effective one.

THE GOVERNMENT'S SECURITY CLASSIFICATION AND DECLASSIFICATION PROGRAM

BY

WILLIAM L. BROWN, Executive Director

In January 1971, the President directed that a review be made of the security classification procedures under Executive Order 10501. A committee was set up under then Assistant Attorney General William Rehnquist to study the existing classification system and to make recommendations with respect to its operation and to propose steps that might be taken to provide speedier declassification. Based upon that review and other studies, a new and progressive Executive Order on the classification and declassification of national security information and material was issued by the President on March 8, 1972. The Order, known as Executive Order 11652, became effective on June 1, 1972. It is important to note that this reform was the first major overhaul of the Government's classification system in 20 years.

The Interagency Classification Review Committee was established to assist the National Security Council in monitoring implementation of the new order and any implementing directives issued by the President through the NSC. The Committee's role as envisioned by the Executive Order was to be a novel one--indeed--a bold one. In years past it had been assumed--or perhaps hoped--that the Government's security classification system would be self-policing. As we all know, that assumption was not borne out. As the President himself stated when he issued the new Executive Order:

"Unfortunately, the system of classification which has evolved in the United States has failed to meet the standards of an open and democratic society, allowing too many papers to be classified for too long a time. The controls which have been imposed on classification authority have proven unworkable, and classification has frequently served to conceal bureaucratic mistakes or to prevent embarrassment to officials and administrations.

"Once locked away in Government files, these papers have accumulated in enormous quantities and have become hidden from public exposure for years, for decades--even for generations."

* * *

"The many abuses of the security system can no longer be tolerated."

* * *

"Yet since the early days of the Republic, Americans have also recognized that the Federal Government is obliged to protect certain information that might otherwise jeopardize the security of the country."

* * *

"Clearly, the two principles of an informed public and of confidentiality within the Government are irreconcilable in their purest forms, and a balance must be struck between them."

Thus, the novelty of the ICRC lay in its role as a Government-wide overseer of the new and more progressive security classification and declassification system established by the Executive Order. The boldness lay in the belief that the Committee could actually perform that function successfully. Time will tell. Some Congressmen are betting that the Committee cannot do it. I am betting that it can. However, it can only do it if professionals like yourselves get enthusiastically behind the program and instill that same enthusiasm in those that work for you.

The ICRC is the first White House level committee with overall responsibility for the Government's security classification program. In addition to its oversight responsibility, the Committee is to receive, consider and take action on suggestions and complaints from persons within or outside the Government with respect to the administration of the Order, and, in consultation with the affected Department or Departments, it is to assure that appropriate action is taken on such suggestions and complaints.

Some three weeks before the Committee first met, a National Security Council directive was issued on May 17, 1972, whereby the President gave more specific directions concerning the implementation of the Executive Order. That directive specified in even more detail the functions of the Committee. The Committee was directed to "place particular emphasis on overseeing compliance with and implementation of the Order and programs established thereunder by each Department." Moreover, the Committee was "to develop means to (a) prevent over-classification, (b) ensure prompt declassification in accord with the provisions of the Order, (c) facilitate access to declassified material and (d) eliminate unauthorized disclosure of classified information." Finally, it was to hear appeals from the denials of declassification requests made under the mandatory declassification review procedures of the Executive Order.

The Committee was initially composed of senior representatives of the Departments of State, Defense, and Justice, the Atomic Energy Commission, the Central Intelligence Agency, and the National Security Council Staff. Subsequently, the Archivist of the United States was added to the Committee membership, and he currently serves, by designation of the President, as the Committee's Acting Chairman. The Committee meets at least once a month in the West Wing of the White House.

In exercising its responsibilities, the Committee steadfastly strives to keep two fundamental goals of the Executive Order in the constant balance mandated by the President; i.e., the legitimate need of protecting information and material which bear directly on the effectiveness of our national defense and the conduct of our foreign relations must be continually balanced with the concept of an informed citizenry in a free society. I am happy to say that under the auspices of the ICRC, significant progress has been made by the Government in achieving these goals. Of course, this is not to say that all the goals have been reached. Far from it! There is still much work to be done and, furthermore, it will always be necessary to exercise an oversight responsibility. However, I am pleased with the progress being made and I can assure you that the ICRC intends to continue vigorously pursuing its oversight responsibilities.

I think that a brief review on how the ICRC carries out its responsibilities will be of interest.

In the beginning, the Committee spent a good deal of its time on two subjects, namely reviewing and approving agency implementing regulations and reviewing appeals from agency denials of declassification requests. In each case, the time was I believe, well spent, for the regulations are now in effect and the Committee has proven itself independent and capable in exercising its appeals responsibilities. The Committee also developed its own appeal procedures which were published in the Federal Register last summer.

In 1972 it appeared to many on the Committee that they would be deluged with appeals. Lengthy discussions took place on how the Committee should cope with this expected flood.

As a matter of fact, the expected deluge of appeals to the Committee never materialized. In part this was because, after a few false

starts, the system proved to be responsive. In part, too, it was because the Committee made its own position quite clear: it was not going to be a rubber-stamp for agency denials. Thus, agencies have approached their responsibilities with an impressive conscientiousness. Between June 1, 1972, when the new Executive Order went into effect, and the end of December 1973, the agencies of the Federal Government acted upon 873 requests for declassification. The overwhelming majority of those have been granted either in full or in part, most of them in full. While we are very pleased with this part of the program, we have been encouraging speedier determinations and, indeed, there has been a great deal of improvement. The Government's experience with the Freedom of Information Act has been that the number of requests from the public have increased each year since the Act became effective. We are beginning to see the same pattern develop with respect to mandatory review requests at the agency level.

The first appeal to reach the Committee--for the "Gaither Report" of 1957--resulted in declassification; the agency's denial was reversed. To date, the Committee has had to deal with only five appeals of denials. That is by no means a deluge, though the time the Committee members spent on each appeal was considerable. That so few appeals have reached the Committee is a tribute both to the willingness of agency officials to make the new system work by making material available and to the vigor with which the ICRC has pressed the new system.

The promulgation of agency regulations and the work of the ICRC in handling appeals under the mandatory review provision of the Executive Order are only part of the story of the Committee's role. At least as important--perhaps, in the long run, more important--is the reporting system which the Committee has developed.

In September 1972 the Chairman of the ICRC, Ambassador Eisenhower, requested the assistance of the National Archives and Records Service in preparing a series of management report forms which could be used by governmental departments in preparing the quarterly reports required by Section X.C. of the National Security Council Directive of May 17, 1972. Suitable report forms were quickly developed by NARS in cooperation with the various interested agencies and they were established as permanent requirements by the ICRC on February 27, 1973. This calendar year quarterly reporting system is the primary means by which the ICRC evaluates departmental compliance with, and implementation of, Executive Order

11652 and the programs established thereunder. The reports are submitted by some 37 agencies and departments within the Executive Branch.

What are these reports? Let me give you a brief outline.

1. Report of Authorized Classifiers. This is a list of people with authority to classify by name and title or by title and organization, and totals for each classification category.
2. Report of Classification Abuses. This is a report of instances of under- or over-classification, unnecessary classification, improper marking or improper exemption from the General Declassification Schedule or other discovered occasions of classification abuse. Abuses are primarily discovered through the use of departmental inspection programs.
3. Report of Mandatory Declassification Review Requests. This is a log-type report of declassification requests made pursuant to Section 5 of the Order reflecting the requester, date of request, subject matter, date and nature of departmental action, costs and other information associated with those requests; and
4. Quarterly Summary Report. This is a statistical summary of the number of documents classified by a department during a quarterly reporting period. Departments, I might add, are also given an opportunity to elaborate on accomplishments in achieving the objectives of Executive Order 11652. Among the things that the Quarterly Summary Report allows the ICRC to do is to see how many classified documents are being exempted from the General Declassification Schedule. This is an area, by the way, that still needs improvement as too many documents are being exempted for insufficient reasons.

As my brief outline indicated, the reports serve as a valuable tool to be used by the ICRC in measuring how well a particular department is doing in implementing the new classification and declassification program. So now, for the first time, someone is in a position to know with reasonable accuracy what agencies are doing--or not doing--in the area of security classification and declassification. To the fullest extent possible, these reports are analyzed each quarter. When a deficiency or other matter requiring improvement are noted, it is brought to the

attention of the responsible department along with a request that the matter be immediately rectified. To the extent possible, the ICRC assists the department in solving the various problems as they develop. At times, this can be a time-consuming process, since several departments have not as yet fully implemented every aspect of the reporting requirements, primarily because of the large volume of material generated together with a lack of manpower and adequate resources. However, steady progress has been made and, indeed, most departments have fully implemented the requirements.

In order to determine the reliability of the statistical information being received through the reporting system, the ICRC recently required reports from each reporting department which describe how various kinds of statistics are developed. For example, since the ICRC allows departments to obtain statistics for these quarterly summary reports by an actual count or by a scientific sampling system, the ICRC required each department using the sampling system so that the ICRC could review it and determine if the system was scientific enough to allow extrapolation of a reliable estimate of what an actual count would be. The same type of request was made for copies of departmental inspection programs which are used to find classification abuses. Where it is determined that a department has an unreliable sampling or inspection program, the department is required to revise its program to meet acceptable standards.

The reports already provide some idea of what is happening, and the picture they give has, overall, been a very pleasing one. The best example is the substantial reduction in the number of persons authorized to classify national security information. This has been a major effort. The total number of authorized classifiers within all departments has been reduced by over 71% since Executive Order 11652 went into effect and this reduction is continuing. The number of classifiers in Government now stands at approximately 17,000 whereas in early 1972 it was 59,316. Percentages of some of the major reductions achieved between the time the Executive Order went into effect and December 31, 1973, are as follows: Agency for International Development and Overseas Private Investment Corporation - 70%, Arms Control & Disarmament Agency - 60%, Civil Service Commission - 79%, Department of Commerce - 99%, Department of Defense - 76%, General Services Administration - 96%, United States Information Agency - 50%, Department of Justice - 54%, National Aeronautics and Space Administration - 61%, Executive Office of the President - 81%,

Department of State - 64%, Department of Transportation - 86%, and the Department of the Treasury - 75%. I think the figures I just gave you all add up to a rather remarkable feat for a bureaucracy which had been marching in the other direction for so long.

Since there is a direct relationship between the number of those who can classify material and the volume of material classified, these figures are especially impressive. We are still classifying a great deal of information, but the volume is now being brought within rational bounds.

Millions of pages are also being declassified in active declassification programs in a number of agencies. The National Archives and the AEC lead the way. Indeed, the bulk of the declassification review of 30-year-old material is being conducted at the National Archives in some instances with the assistance of Agency personnel specifically assigned to this project. The goal of this program is to review by 1975 all of the permanently valuable records of the Federal Government which were created during World War II and earlier periods. As of today, the National Archives has declassified over 75 million pages, including declassification carried out at the Roosevelt, Truman, Eisenhower, and Kennedy Presidential Libraries. That active declassification program is continuing.

Other agencies have conducted their own comprehensive declassification reviews. Most notable the Atomic Energy Commission has declassified over 1.2 million documents of the over 2.2 million documents reviewed since their classification review program began several years ago. The Defense Department has reduced its Top Secret document inventory by 25% and has taken action to develop guidelines for blanket declassification or downgrading of DOD records which are over 20 years old. The Defense Department has also initiated action to introduce into NATO an automatic downgrading and declassification system patterned after that established by Executive Order 11652. During 1973 the State Department published five volumes in the series "Foreign Relations of the United States" resulting in declassification of approximately 8,000 high level documents on American foreign policy in 1947 and 1948. These and other agency declassification programs reflect the commitment of the agencies to make the new classification and declassification program work.

The quarterly reporting of classification abuses is also useful. It reflects certain trends with respect to the types of classification abuses committed. We have found that abuses are committed

primarily in the following areas: (1) improper classification, (2) failure to properly mark a document with the stamps appropriate for assigned classification and for the assigned declassification schedule or exemption therefrom, and (3) the unauthorized use of classification authority.

Departments are required to take action to correct classification abuses when they become known by notifying the responsible employees that their actions are in violation of Executive Order 11652 and the implementing NSC Directive. Repeated abuses are grounds for an administrative reprimand. One very effective way to lower the number of classification is through the use of frequent and w orientation and training programs. The iated such programs and has encoura, encies to do the same. Such programs ha effectively used by a number of the rep and departments. It is important that these programs impress on each authorized classifier his or her new and personal responsibility with respect to classification decisions and impress upon them the fact that sloppy classification practices can no longer be tolerated. I cannot stress the importance of this statement enough except to say it again. Sloppy classification practices can no longer be tolerated.

Our unauthorized disclosures reports indicated that there was a very limited number of important unauthorized disclosures of classified information during calendar year 1975--10 to be exact. None involved Top Secret information. The disclosures consisted exclusively of leaks to the press. While any unauthorized disclosure of classified information is a serious matter, there are firm grounds for confidence that one of the primary goals of the Executive Order is being achieved, i.e., the protection of information or material which bears directly on the effectiveness of our national defense and the conduct of our foreign relations.

One especially noteworthy and innovative right given by the Executive Order is the right of mandatory review which I touched on earlier. This is a right which allows any member of the public or any governmental department to make a mandatory declassification review request of classified information or material over 10 years old provided that the information or material is described with sufficient particularity to allow the requested agency to identify and find it and provided that the request is not unduly burdensome. This right of mandatory review is a major progressive step forward in meeting one of the primary goals of Executive Order 11652 which is

to make information regarding the affairs of Government readily available to the public.

I have already indicated the Government's success in this area, but I would like to add one more item. In order to make this new and important right better known to the public the ICRC has published a pamphlet entitled Know Your Rights to Mandatory Review of Classified Documents. Numerous copies of the pamphlet have been furnished to all agencies dealing with classified information and to members of the public. The pamphlet is an informative reply to a request to an agency for information on mandatory review rights. The ICRC has suggested that when a Freedom of Information Act request is turned down by an agency because the requested document is classified, an insert such as this ICRC pamphlet in any turnaround response would be an ideal way to meaningfully comply with the spirit of the Executive Order and implementing NSC Directive. The first printing of this pamphlet (some 15,000 copies) is all but done, and a second printing is now in the works.

The ICRC, I think, has made its belief clear that a reduction in the number of documents classified is one indication of agency good faith in complying with Executive Order 11652. Consequently, it has encouraged such reductions in the firm belief that a tighter classification system consistent with the requirements of the Executive Order is a better system and one more in the interest of the national security as well as in the interest of an informed citizenry. This tighter system is mandated by the Order's limited definitions of each of the three classification categories of Top Secret, Secret, and Confidential and by the prohibition against classification for purposes other than national security purposes. The Order specifically states that in no case shall information be classified in order to conceal inefficiency or administrative errors, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the legitimate interest of national security. The classification stamp must be used with judicious restraint. I firmly believe that it is in the real interest of the national security to have a tight system which commands the respect of all who work with it. Executive Order 11652 when fully implemented will be such a system.

The second quarter of calendar year 1973 was the first quarter for which the ICRC has complete

figures on the number of documents classified by most departments. While it is too early to see if a definite downward trend has been established, the Committee has been informed by several agencies that they estimate that there have been marked reductions in the number of documents classified from years past. The AEC, for example, shows an 83% reduction in the number of documents classified Top Secret in 1973. The USIA estimates that 30% fewer documents were classified in 1973 than in 1972. There are good grounds for hope that as time goes on the statistics will demonstrate a progressive reduction in classified material and greater agency control over it.

All departments having classification authority were required by the NSC Directive to undertake the establishment of a data index system no later than July 1, 1973, for Top Secret, Secret, and Confidential information in selected categories approved by the ICRC as having sufficient historical or other value appropriate for preservation. The system is required to index the selected categories of information and material produced and classified after December 31, 1972. Detailed instructions on how to set up the data index were issued January 23, 1973. Most agency systems are fully operational. While a few are still being developed the results, so far, are encouraging. However, this system is not nor was it ever intended to be a panacea. It does, however, have a number of useful purposes particularly for those smaller agencies who index 100% of their classified material. It is also particularly useful for information retrieval purposes.

Since attending my first ICRC meeting in the Roosevelt Room at the White House last summer, I have been very impressed by the good sense, good will, and firm dedication of the Committee's members. Executive Order 11652 charted a new and progressive course which the Committee has generally followed with an impressive tenacity resulting in real progress. The Committee's Annual Progress Report was recently publicly released by the White House Press Office. Upon its release, Gerald Warren, Deputy Press Secretary, said that the President continues to take an active interest in this program and he is quite pleased with the progress being made by the Committee. However, like anything else, progress has to continue or you lose ground. The Committee thus has every intention of continuing its implementation of this new and progressive program.

There is a bronze plaque on the wall of the Roosevelt Room in which we meet honoring F.D.R. As you know, he always loved the sea and sailing.

On it there is a motto which was once called to my attention. It is a quotation from the Roman philosopher Seneca; he said: "I will hold my rudder true." This is precisely what the ICRC has been doing. And, ladies and gentlemen, in a bureaucracy as large as the Federal Government's--that is no mean achievement.

Thank you very much.

QUESTIONS AND ANSWERS

MR. CHELIUS: During the appeals process, does a representative from the agency who is denied the request disqualify himself from voting?

MR. BROWN: Ordinarily when an appeal, or when a request, a mandatory review request, is made, it goes to the department on the operational level that originally handled the material or is responsible for the information contained in the material.

When an individual is turned down, it then is appealed to Departmental Review Committee. Now, the committee is set up with senior agency officials. To my knowledge, these officials usually are not in on the initial decision, and if the appeal is subsequently turned down at the departmental committee level, it can be appealed to the ICRC, but, so far as I know, there's been no conflict.

MR. ROBINSON: Jack Robinson from CNA, and I would like to ask a question.

One of the reports that you require is on abuses, and you have commented that there have been some reported. It's a little hard to visualize calling the shots on yourself and I was just wondering the view of the committee as to what has been reported.

Could you give us some idea of perhaps numbers--if those are not improper to comment on--and some of the of like, the DoD say, "By the way, we did make some abuses and we did this last week, and we shouldn't have."

MR. BROWN: Well, as you can imagine, this is a problem getting people to report on themselves, getting departments to report abuses to higher levels. Many agencies are doing it. Some are not doing it so well. There's a lot of improvement that needs to be made in the reporting of classificational abuses, but I think as time goes on and as the agencies become used to the system, they will report more and more abuses.

I think it's more of a reflection on an agency to report no abuses than to report abuses, because we know there are abuses. If they're not being reported, they're not doing their job.

Furthermore, Congress has expressed interest in this. The Muskie Committee recently asked for copies of all the reports of classification abuses. We've got a similar request for the Moorehead Committee, so I think it's going to be incumbent upon every agency to be honest and straightforward in reporting the abuses.

I think the best way to find abuses in the way that the ICRC has set up and that is for the agencies to have departmental inspection programs and have good programs that can report these abuses to the committee.

MR. FLORENCE: This is Bill Florence, Consultant. My question goes to the degree of progress that I'm hearing so many statements about recently, today's luncheon talk, and your talk, and I have in mind a figure of the number of top secret documents that--cited as representing a degree of progress, and implementing Executive Order 11652. The Department of Defense has stated that they have five hundred and forty-one thousand five hundred and thirty-nine documents marked Top Secret.

Now, by your Executive Order definition, this means that each and every one of those documents subjected to unauthorized disclosure will cause exceptionally grave damage to this nation, not just grave damage, but exceptionally grave damage, and my question is: At what point in time would you consider that you have reached the goal of only top secret information being in those documents that were treated, qualified? For the point is, I don't think that the country could stand five hundred forty-one thousand exceptionally grave damages.

There must be some place here where there's an excessive number of documents, and I just wonder if this is the sort of a criteria that you might have in mind here as to a certain amount of progress made, to say, "We've got there."

MR. BROWN: As I indicated, we have made progress and we've made significant progress, but you know it's like anything else, the job is never done.

I've also indicated that it will require continuing oversight. As long as you have human beings working with the program, you're going to have fallacies; you're going to have abuses, and whatnot, but as long as we can continue to have an oversight responsibility and to cut down on

these fallacies and these abuses to the extent we can, I think we'll be in good shape.

Now, I don't know about whether this five hundred thousand documents of the department are legitimately classified top secret or not. I would assume they are. As Joe Liebling pointed out, there are over three million people within the Department of Defense. There are a lot of documents being classified, but I am also sure that there are a lot of documents right now in the Department of Defense that have been improperly classified, but the important point I think is that they have recognized this. The policy makers in the Department of Defense have started off on the right track. They're getting the word out.

One way they're getting the word out is by the very fact that Joe Liebling appeared here today and told you what their policy is, and I think they are making progress.

Now, perhaps as to the specifics on it, Joe or Art VanCook could comment.

MR. VAN COOK: I'm Art VanCook, Director, Information Security Division, Office of Deputy Assistant Secretary of Defense. I want to talk about the five hundred and forty-one thousand five hundred and thirty-nine documents that Bill alluded to.

He knows as well as many of us here that we have to be talking about information rather than we do documents. Now, one piece of information that's generated at the National Security Council level to get to the Department of Defense worldwide may result in the creation of ten thousand documents, but in those ten thousand documents is the same piece of information. So it's not that we have five hundred and forty-one thousand five hundred and thirty-nine separate pieces of information. We do have five hundred forty-one thousand five hundred thirty-nine originals and copies thereof; how many originals, I don't know, but just to conduct the Department of Defense business, we have to get these documents disseminated on a worldwide basis.

Now, how much information we're talking about that's in the top secret category, I can't tell you, but we do have safeguarding procedures established in both the Department of Defense and defense industry which are designed to protect these individual pieces of paper.

I think you should have no fear that we've got five hundred and forty-one thousand or a half

a million documents kicking around, floating. Each and every one is under some stringent safeguarding procedures, and we've had--I don't know of any unauthorized disclosures in the Top Secret classification category within the past year or two years or three, or whatever so I think we have to be talking more on information than we should be talking about pieces of information which are lying around in safes.

The point is, that we are working toward reducing our classified inventories, in this case, a reduction of twenty-five percent, to eliminate or to reduce the hazard of unauthorized disclosure.

MR. FLORENCE: May I follow through just to be sure I've got the answer to the question I asked?

I think I do have the answer, that the representation of using documentation of five hundred forty-one thousand is not itself any degree or indication of reducing classification of information.

MR. CHELIUS: I think--I'm not sure--I think that's a misleading statement, Bill.

MR. FLORENCE: It's a question of if that is an indication of reducing the classification of information, then Mr. VanCook seems to be a little bit out of sympathy with the idea.

Mr. VanCook said that you've got to put your mind on the information aspects of the classification method, not on the number of documents, and so I will ask if Mr. VanCook will answer then: Isn't the information aspect of what we're talking about the important thing and not the number of vehicles called documents that carry that information?

MR. CHELIUS: Art?

MR. LIEBLING: May I ask a question, please?

MR. CHELIUS: Mr. Liebling, the Office of the Assistant Secretary of Defense.

MR. LIEBLING: Are you talking about the fact, Bill, that the half-million was excessive or that they may be overclassified?

MR. FLORENCE: My question now is that the representation of a reduction of the number of documents does not--as far as I can tell--show a reduction of the classification of information. This was represented as being "We're making progress in declassification." We're making progress in hearing classification of information, because we got five hundred forty-one thousand documents."

Now, I ask about the five hundred forty-one thousand documents and I'm told just the information is important, that these five hundred forty-one thousand may be many, many copies of the same item of information.

MR. LIEBLING: That's correct. One, you gave an indication that we have twenty-five percent reduction. Now, within that reduction, it can be a downgrading or elimination from inventory. Now, the degree, of course, we don't know, because we don't have total numbers.

Now, as you said, "as far as you can determine." How can you know if you do not have access to those documents at all?

We've indicated a twenty-five percent reduction and all we're portraying is the fact of a progressive action. We're not saying we have a utopian solution to the problem at all. There isn't any speaker yet in the last four years who has said that.

DOD PANEL--PROGRESS AND EFFECTS OF IMPLEMENTATION OF EXECUTIVE ORDER 11652

MR. ARTHUR VAN COOK, Moderator
Director, Information Security Division
Office of Deputy Assistant Secretary of Defense (Security Policy)
Office of Assistant Secretary of Defense (Comptroller)

LT. COL. CHARLES T. GRIMES, USA, Panelist
Office of Assistant Chief of Staff for Intelligence
Department of the Army

MR. FRANK LARSEN, Panelist
Head, Security Review and Classification Section
Office of Chief of Naval Operations
Department of the Navy

MR. LAWRENCE MYERS
Chief, Classification and Information Security Branch
Headquarters, USAF

PRESENTATION BY MR. VAN COOK

It is my pleasure to again appear before this audience. Mr. Liebling, in his presentation this afternoon, covered generally the highlights of the progress of the Department of Defense since promulgation of Executive Order 11652. I am joined here this afternoon with Larry Myers of the Department of the Air Force, Frank Larsen of the Department of the Navy and Col. Grimes of the Department of the Army. It is our intent to familiarize you with results of certain programs which show conclusively that

the Department of Defense Information Security Program is being carried out with a high degree of initiative and effectiveness.

I deal with the members of this Panel directly on an every day basis. Since I have been assigned as Director of Information Security, I have enjoyed a close working relationship with them and they have cooperated fully with me and members of my staff. I take this opportunity to express my appreciation to each of them. They are prepared to expand on certain portions of my presentation and to be responsive to your questions concerning any and all portions.

From the outset of the establishment of the Information Security Program, top level management in the Department of Defense has emphasized the need for immediate and effective implementation and has called for maximum support and continuous monitorship on the part of command and supervisory officials at all levels throughout the Department. To assist in obtaining assurance that this was being accomplished, Mr. Liebling on June 13, 1972, established an Evaluation Division in his office. This Division is charged with the responsibility for monitorship of the Department of Defense Information Security Program through inspection and reporting. Since its establishment, members of this Division have conducted reviews of the Information Security Program at major DoD component headquarters and at major Defense Contract facilities throughout the United States.

The Information Security Program reviews and inspections conducted by the Evaluation Division have proved beneficial in identifying both positive and negative aspects of program implementation and are one of our most effective monitorship tools at the Departmental level. Besides their value in identifying trends, they also bring to our attention the development of novel and innovative approaches within various DoD components which are designed to increase the effectiveness of Program implementation.

To ensure that effective monitorship programs are in being within components as well as at the Departmental level, the senior officials of all DoD components, who are responsible for the Information Security Program were requested to provide an analysis of the inspection programs conducted in their respective components during the period June 1, 1972 through December 31, 1973.

Review of DoD component self-inspection reports indicated that during the period June 1, 1972 through December 31, 1973, over 2500 formal

inspections were conducted within the DoD components. In addition, approximately 10,000 informal reviews and security assistance visits were conducted during the same period. As a result of these inspections and reviews, significant reductions have been made in the numbers of classified documents held in component inventories. For example, in one major component, an 88% reduction in classified holdings has been achieved. These reductions, in turn, have resulted in the reduction of the physical storage facilities required and have improved the security of that classified information remaining in inventory by consolidation of resources. Concomitantly, components have reported a notable reduction in administrative security violations by as much as 43% in some activities. The foregoing results are positive manifestations of effective monitorship and implementation of the Information Security Program in the Department of Defense.

To make Program reviews and inspections more effective, an inspection checklist was developed which is comprised of 83 questions, each referenced to specific and pertinent portions of DoD Regulation 5200.1-R. Program reviews have shown that the checklist is being widely used by components as an educational tool and in the inspection programs.

We have closely examined the results of the Program reviews conducted in component headquarters. Where deficiencies have been identified; component senior officials have been requested to take necessary corrective action and to report when such action has been accomplished. In addition, component senior officials are made aware of the innovative approaches to effective implementation developed by other activities and are encouraged to adopt similar procedures where feasible.

One of the most recent significant follow-on monitorship activities has been a project to review the implementation of the Information Security Program within the major activities of the Office of the Secretary of Defense. This action could have a significant impact on achieving the goals established by the President in Executive Order 11652 because it is at the highest Departmental levels where control and curtailment of classifications and exemptions can have the most significant influence on the volume of classified documents created.

In conjunction with the establishment of monitorship programs, the Assistant Secretary of Defense (Comptroller) has directed that the designation

of classification authorities will be limited to the minimum number of absolutely required for efficient administration. Since the issuance of Executive Order 11652, the Department of Defense has reduced Top Secret classification authorities from 803 to 591, Secret classification authorities from 6,884 to 3,025 and Confidential authorities from 23,361 to 3,417. The latest total of 7,033 classification authorities represents a net reduction of 24,015 classification authorities, or approximately a 77% reduction from the number of officials previously authorized to classify information under Executive Order 10501, as amended.

The Department of Defense has also directed continuing action toward limiting the use of Exemption Authority within the Department. To this end, the Assistant Secretary of Defense (Comptroller) called for the detailed review of classified information by responsible officials to ensure that, on every item of that information, the classification levels assigned and dates or events for downgrading and declassification are the minimum consistent with the interests of national security.

To complement this action, the Assistant Secretary of Defense (Comptroller) on October 18, 1973, in a memorandum to the heads of all DoD components, directed that during the period November 1, 1973 through October 31, 1974, a mandatory review of all security classification guidance issued by or under the auspices of their respective components be conducted and the results of that review be provided to his office on a quarterly basis.

The results of the review conducted by components for the first two quarters under this program have been examined. These results indicate that 9,916 Program/System/Project security classification guides and Contract Security Classification Specifications were reviewed.

Of these, 23% were revised to cause earlier downgrading and declassification and 10.5% were revised to cause fewer exemptions from the General Declassification Schedule. In other words, over 3300 classification guides and Contract Security Classification Specifications were revised to accelerate the downgrading and declassification process. The significance of this action is that the revision of these guidances, in turn, will cause earlier downgrading and declassification of hundreds of thousands of documents which are already classified on the basis of the original guidance and will eliminate the unnecessary classification of a like amount of documents to be created in the

future which deal with information related to that covered by the revised guidance.

As a by product of this review and report, the following significant benefits were gained:

- Many technical characteristics of seven missile systems, one radar system and 126 ordnance systems were downgraded and the fiscal data relating to these latter systems was declassified. In addition, 10 air weapon systems were totally or partially downgraded and the hardware of two electronic systems was declassified.
- One activity reported that 68,346 classified maps and associated documents were declassified, 14,000 were downgraded to Confidential and 19,300 downgraded to Secret. The reduction in requirements associated with the protection of these documents such as handling, transmission and accountability, resulted in a cost avoidance of approximately \$22,800. In addition, 387 tons of Confidential material and 111,600 Secret documents were destroyed in this same activity.
- Downgrading and declassification action on one classified Project resulted in an estimated cost avoidance of approximately \$100,000.

In a separate action, Mr. Lieblich in August 1972, initiated a project to review for downgrading and declassification Military Standardization Handbook 140C, Security Classification and Cognizant Activity of Electronic Equipment. This handbook lists over 100,000 separate items of standardized electronic equipment both classified and unclassified.

The results of this review completed on March 31, 1973, show that of the 7,338 classified items contained in the Handbook, total declassification was accomplished for 2,350 of them. This represents a 32% reduction in classification. Action on this project is continuing to determine statistics on the number of pieces of hardware and documentation such as technical and modification work orders that have been declassified as a result of this action. Initial results indicate that literally hundreds of thousands of sets, component parts, spare parts and technical and modification work orders will be declassified.

In support of the President's program for the declassification and release of historical records, the Deputy Secretary of Defense approved guidelines to authorize blanket declassification of the great majority of the Department's official records dated prior to July 1, 1950. Declassification teams of major components are engaged in

the review of this material and thus far, have reviewed and approved for declassification within the Department over 110,000 linear feet of classified records. The Archivist of the United States has been authorized by the Secretary to apply these guidelines to Defense records held in his custody. Through the application of the Defense guidelines to these records, the National Archives and Records Service, in cooperation with the Department of Defense, has declassified approximately 50,000,000 pages. A study is currently being conducted to determine whether it is feasible to apply similar guidelines for the declassification of official Departmental records as they become 20 years old.

At the Department's request, the United States delegation to the NATO Security Committee submitted a Defense developed proposal to that Committee to incorporate within NATO, a classification management program similar to that which is in use throughout the Department of Defense and which is based on the provisions of Executive Order 11652.

If adopted, this proposal will provide, for the first time, an automatic downgrading and declassification system within NATO.

Concurrent with the actions thus far described, the Department of Defense has been actively engaged in developing ways and means of reducing classified inventories and in gathering statistical data in order to establish a statistical base against which to measure program progress with a higher degree of accuracy.

For example, on December 14, 1972, the Deputy Secretary of Defense directed the heads of all Department of Defense components to conduct a Top Secret inventory reduction project within their respective activities during the period February 1, 1973 through March 31, 1973.

Reported results of this project showed that the Department of Defense met the established 25% reduction goal. By March 31, 1973, 180,469 documents were eliminated from the Top Secret inventory leaving a total of 541,539. This was accomplished generally by the destruction.

The results of this program show that the task of weeding out non-record material which serves no useful purpose can be accomplished. Department of Defense components have been urged by top level management to continually examine classified material in files and storage areas with a view to declassifying, downgrading, destroying

and transferring it to Federal Records Centers in order to reduce the classified inventory to the maximum consistent with operation and national security requirements. The Department's Information Security Program managers plan to conduct another such program during this calendar year.

To have more definitive data available regarding the classified inventory of Defense Industrial facilities, the Defense Contract Administration Services was directed to conduct a survey of all industrial facilities under its cognizance to obtain data on the volume of classified documents received, generated, transmitted or referred outside the facility, destroyed, declassified and held in inventory in the various classification categories for Fiscal Year 72.

The survey showed that the beginning FY 72 inventory was comprised of 15,390,167 classified documents. The inventory at the end of FY 72 showed a total of 13,876,192 classified documents; a net reduction of 1,513,675 classified documents or 10% of the beginning inventory. The results of this survey are a good indication that industry, consistent with good records management practices, is progressively reducing its classified inventory.

In connection with quarterly reports, extensive effort has been expended by the Department in an effort to develop viable sampling techniques which will provide the Interagency Classification Review Committee with a reliable estimate of classification/downgrading/declassification actions of the Department worldwide. On April 5, 1973, the Assistant Secretary of Defense (Comptroller) requested the heads of the Military Departments to conduct a survey of at least two activities in their respective services during the period May 1 through May 31, 1973.

A total of seventy-five (75) activities were selected by the Military Departments for the conduct of the survey. The results showed that approximately 7% of the information created in the surveyed activities was being placed in the Advanced Declassification Schedule, 42% in the General Declassification Schedule, 42% exempted from the General Declassification Schedule, and 7% excluded. The higher than desired exemption rate may be explained by the fact that many of the selected activities were heavily involved in intelligence and communications activities. Despite this fact, the results do provide an accurate base against which to measure program progress in the same activities. To achieve this end, the heads of the Military Departments were requested to conduct, during the period

May 1 - May 31, 1974, another survey of the same activities which were selected last year.

To be more responsive to the requirements of the Quarterly Summary Report to the Interagency Classification Review Committee, the Department has also utilized statistical data developed by the Defense Communications Agency through the Switch Network Automatic Profile System (SNAPS). This is an established automated sampling system for the gathering of data on the total number of messages processed through 19 switch network communications centers worldwide. As presently established, the system allows the Department to report, on a quarterly basis, the total number of messages generated throughout the Department by classification category. For example, during the period September 1, 1973 through November 30, 1973, there were 6,750 Top Secret, 223,250 Secret and 659,400 Confidential messages processed in worldwide communications centers. It should be pointed out that only 5% of the total message traffic processed is classified.

To improve on this presently established sampling system and thereby be more responsive to Interagency Classification Review Committee requirements, the Assistant Secretary of Defense (Comptroller) requested the Defense Communications Agency to conduct a feasibility study to determine the mechanics and lead-time requirements for modification of the Switch Network Automatic Profile System to permit the gathering of statistical data regarding the downgrading/ declassification/exemption status of all classified messages. That study was recently completed and the results showed that the gathering of the data is feasible. Consequently, the added sampling requirement was levied on the Defense Communications Agency and the first quarterly report is due to be submitted in July 1974.

The Department of Defense undertook to establish a data index system in accordance with the provisions of the May 17, 1972 National Security Council Directive. It was decided that initial Data Index System actions by the Department should be taken on a selective basis in a few key components. To this end, the already automated Documents Control System in the Office of the Joint Chiefs of Staff, the Defense Documentation Center System and the Documents Indexing System in the Defense Communications Agency have been designated as the data bases for initial Data Index System implementation. Should the initial phase of implementation prove to be practical and economical, the system will be extended throughout Headquarters offices in the National Capital Region.

After more than a year's experience with the Information Security Program and based on the results of Departmental Program reviews, it became evident that certain changes were required in the Department's implementing regulation to improve its effectiveness.

For example, experience taught us that changes were required to be made to the regulation to re-institute the former Group 3 provision for automatic downgrading. A change was, therefore, made to the regulation which prescribes that former Group 3 material shall be downgraded at 12 year intervals but not automatically declassified. This action will, through downgrading, remove numerous documents from the requirements of annual inventory and at the same time, will assist in ensuring that new documents deriving their classification from this category of documents are classified at levels consistent with current national security interests.

Another major change was adopted which was designed to accelerate declassification of information and material and minimize exemptions. Departmental Program Reviews and comments from the field indicated that more information was being exempted under the category 3 provisions of the Executive Order than was believed necessary. By placing information in this category, classification would be maintained for periods up to 30 years from the date of origin. To accelerate declassification, the regulation was changed to provide that information placed in exemption category 3 concerning scientific and technical matters, installations, programs and the like shall be automatically declassified at the end of 15 calendar years. This is a progressive action which should force Top Secret Classification Authorities to more closely examine information being placed in this Exemption category.

In addition to these major changes, other substantive changes were adopted which impose more restrictive guidelines for the designation of original classification authority who authorized, approved or sanctioned exemptions called for in a classification guide to be placed on the document. This latter change will allow speedier identification of the exemptor when a question arises as to overuse of exemption authority.

Because of the number of these and editorial changes involved, it was decided to publish a complete reissuance of DoD Regulation 5200.1-R.

The ultimate success of any Information Security Program depends upon the individual - his

motivation, his dedication and his knowledge and familiarity with Information Security practices, policies and procedures.

Recognizing the importance of this "keystone" element, both the Office of the Secretary of Defense and the Defense components have taken positive steps toward educating military and civilian personnel at all levels of command and supervision to assure full understanding and compliance with the Executive Order, the National Security Council Directive and the Department's implementing regulation. In this regard, regulatory issuances, presentations, video tapes, articles and publications have been used to advantage.

Since the date of promulgation of the Executive Order, the Deputy Assistant Secretary of Defense (Security Policy) and senior representatives of his office have participated in numerous national security seminars and symposia such as this. It has been repeatedly emphasized at these gatherings that the overriding objective of the Executive Order is to make more information on government affairs more readily available to the public. Moreover, attendees have been consistently urged to become personally involved in the Program and to challenge government classifications when they felt that overclassification or unnecessary classification was involved.

Within the components, in addition to formal classroom instructions, security managers use security briefings, conferences, security newsletters, bulletins and security assistance visits to enhance the quality of the instruction.

Ongoing planning within components includes the development of specific programs to include (1) Information Security Training at Service Schools, (2) the development of methods and training aids designed to assist action officers, clerks, typists and secretaries in applying classification/downgrading/declassification markings, (3) special educational needs based upon the findings of component inspection programs and (4) Information Security training of reserve personnel in order to use their services, in turn, as instructors in the field during their annual two weeks active duty training.

Finally, in the education and training field, the Department has established an Information Security Management Course at the Defense Industrial Security Institute. This course, of two weeks duration, will be available for both Government and Defense Contractor security management personnel. Its purpose is to provide these personnel a comprehensive understanding and

interpretation of the Information Security Program with particular emphasis on proper classification of information in the interests of national security; progressive downgrading and declassification; and safeguarding of classified information against unauthorized disclosure. This all encompassing course should materially assist personnel in implementing and monitoring the Department's Information Security Program at command and organizational levels and in satisfying command/supervisory responsibilities for effective compliance with Program requirements.

The "pilot" class for this course was conducted in June 1974. Attendance at this class was limited to invited representatives who were, themselves, knowledgeable of the subject matter and who could, therefore, provide valid comments for improvement of subject matter or manner of presentation in future classes. Their comments are currently being evaluated. Seven classes are scheduled for FY 75. During FY 76, a traveling team will be established to present the class at various Government and Defense Contractor activities throughout the United States.

PRESENTATION BY LT. COL. GRIMES

I'm Lt. Col. Grimes and I represent the office of the Assistant Chief of Staff, Department of the Army.

Gene, if you can get Gen. Abrams to sign a general order confirming this (pointing to the rank of Colonel on his name plate), I'd be forever grateful.

Mr. Brown was speaking today about the Interagency Classification Review Committee, and I'd like to reemphasize some of the things that he told you.

Freedom of Information, FOI, as we call it, is personal to me, because I'm also the Secretary of the Army Classification Review Committee. I wish I could tell you that we haven't been inundated with appeals for information, but we have.

We haven't had a lot of appeals, but the quality and the quantity is staggering.

In fact, Friday, just before I left to come down here, I finished a thirty-volume history of the Counter Intelligence Corps, it covered the period 1918 through the Korean War. It was like trying to declassify the Encyclopedia Britannica.

It's just amazing, and it's all being done for one individual. This gentleman is going to receive a sanitized copy of the history. I don't think everyone here is aware that this is a requirement, in the Army.

If an individual requests a document, and we can't give it to him because of classification, we are required to sanitize it; in other words, remove that which is exempt and provide him with the information that is unclassified. This is a horrendous problem. I personally spent two weeks standing in front of a Xerox machine reproducing this document and I can assure you it is a terrible problem, because we are just not staffed for it. This added burden had to be performed in addition to my normal duties as a Department of the Army Information Security Staff Officer. There are two of us providing this service within the Army and it is a tremendous--and I repeat that--a tremendous burden, but it is being done and it is being done in light of and in accordance with the guidance given by the President. We are all, I think, trying to get as much information to the public as possible.

We had another individual who came in and appealed, one appeal, eighty documents. Now, I'm not speaking about four or five pages per document. I'm speaking about area studies on Hungary, studies on Japan, area studies on China, and several other countries all of which are classified.

This material must be sanitized, and this is a very difficult problem. In many instances, there is State Department, JCS and intelligence material incorporated in each volume so there's the additional problem of coordinating with these agencies. The job, however, is being done; it's a little slow in some instances, but everybody is trying very hard. What I'm saying is that I support Mr. Brown's position. We down at the working level, are definitely, behind the effort. The reason I bring this out is because the next topic that I want to discuss with you is the reduction in the number of classification authorities.

In the Army a year and a half ago, we had over thirteen thousand authorized classifiers. The most recent report that I submitted this past Friday shows us below three thousand.

We now have only fifty-three positions in the Army that are authorized to exempt material. That is not very many, and what it really boils down to is that the action officer must go through his boss to a TOP SECRET authority to obtain document exemption. This is often difficult, so what does he do? He uses outdated instructions on the material to be classified. The result is that you may receive improper guidance from your contracting officer. We cannot look at each contract--it would be impossible for us, but you can. In Regulation 5200.1-R, there is a requirement that allows anyone who receives a document on which the classification or the downgrading is questionable, to go

back to the originator, or to the contracting official for further guidance.

I know this does not set too well with the people that are out there in industry. They think this is going to jeopardize their contract. But I think if you go back and say, "look, we're questioning under paragraph such-and-such of the regulation," you will be doing exactly what Mr. Liebling wants you to do. If you don't get any reaction to your question within thirty days, I guarantee that if you write to us you will get action. I think that Ed Reiss here can verify that. His boss is quite interested in the authorities and in the downgrading instructions that are on AMC contracts.

Ed is with AMC, by the way.

I have seen letters that were sent out by Hq. AMC stressing such action by their subordinates. Now, if you cooperate, here is a way in which you can help us to do what the President would like us to do. It gives you, if you will, a little clout. You can question the classification--or the downgrading of a document; by that, I mean, has it, in fact, gone before a Top Secret Authority, or is this just a contracting officer's opinion? If it is, then he has violated the Security Regulation, and we would like to know about it. I'm sure Mr. Brown would, too. Remember that this response is supposed to be provided to you within thirty days. If you haven't received it within a reasonable amount of time, I'm sure that if you put a little note on it and fire a copy of that up to us, we'll get a reply pretty quickly.

That's really all I have, I don't want to repeat what Mr. Van Cook has already said, so we'll leave it open to questions.

PRESENTATION BY MR. LARSEN

Progress is the theme, and if you'll remember, last year Dan Dinan reported to you that as a result of the Naval Inspector General's review of the offices of CNO, some rather serious discrepancies (which were no surprise) existed regarding our classification management program.

As a result of his report, which was approved by the Chief of Naval Operations, we had a charter to move out and do something about control and make progress with a good classification management program in the Navy, and I'm here today to very briefly try and report what we feel are some of our successes in this regard.

Success is kind of a relative thing. I'm reminded of the two gals who competed throughout the years

with each other about the success of their son's male offspring. They hadn't seen each other for a while and recently they met on the street.

The first lady said, "Sarah, I can hardly wait to tell you about how my boy got into psychiatry and in the last two years since I've seen you he's made such a success, he just bought a three hundred thousand dollar home overlooking Malibu Beach high on the hill."

The second lady replied, "Well, you know, a couple of years ago, we were disturbed to find out Timmy was a homosexual, but, you know, recently he just moved in with some doctor who bought a three hundred thousand dollar house in --" (Laughter.)

Actually, what the Naval Inspector General did, and the Vice-Chief of Naval operations, Admiral Holloway, was help us change our approach from chasing situations to evaluating the overall program. He told us to do four things, and these things we have done.

Very briefly, they are, first of all, the Director of Naval Intelligence, under whose command our shop is, was to put out information to our program managers and project officers on how to prepare a classification guide. This we have done. I can report to you that that's dated the 10th of April of this year.

We also identified the CNO office of responsibility for all our classified programs. This was never done before. This we have done.

Over Admiral Holloway's decision, he directed that we increase the educational effort. This we are doing, not only in support of the DoD school, the new one down at DISI, but also in training our reserves so that we are going to have more individual programs available around the country.

In support of the DoD monitoring effort, we pay particular attention to the specifics of the information program on command inspections at all levels, but most importantly OOO9D, which is the shop I come from, has the specific task of monitoring classification guides and reporting to the Chief of Naval Operations on a semiannual basis of any deficiency.

This resulted, from an identity of about a hundred and twenty-five guides a year ago, to almost three hundred today. It's amazing how they come out of the woodwork once you start tracking them down, and it does mean by the end of this calendar year we have every expectation of having all those guides current.

This, from a former forty percent coverage and a ten percent currency, hopefully, by the end of the calendar year 1974, all will be current at the program project officer level on all classified programs in the Navy, including communication systems and intelligence.

We found that basically in the Navy, we have a triangle kind of program. Basic guidance, initial guidance comes from CNO. Then it goes to the procurement activities, which is of primary interest to you folks not in government, for procurement of hardware and then comes back to CNO for operational and tactical guidance.

Well, our procurement activities have done such a fine job for so many years without the basic guidance, and things got into the fleet without anything more than what came out of contracting activities.

We're trying to close each end of that triangle so that it is a workable situation from life to death of the system so that's what we're working for. That's what we've done, and, now, as Dan did last year, I'll give you something else to think about that we're looking at. We just decided to do it last week as a matter of fact.

We want to computerize all our guides so that we can get a print-out by systems, a print-out by command, a print-out almost immediately, as well as a master within our own office to make changes.

This--we feel that if we can keep current--will solve some of the security review problems and also allow us to make more rapid changes and increase the consistency of guides within general areas such as missiles, and so forth.

That's your report from the Navy.

PRESENTATION BY MR. MYERS

I'm not going to make any claim that the Air Force is doing a perfect or a superlative job. For one thing, we've got Hughes and Boeing and McDonnell Douglas and General Electric and many others out here who might like to contest any claims of perfection. Also, the NCMS is mainly contractors and I've sometimes observed that three hundred sixty-two days of the year, the contractor is in a rough position: DoD writes the guides and the contractor has to live with them. But the other three days, when you're here, you have a different role: all you have to do is attack the guides; we have to defend them.

So, I won't claim that we're doing a perfect job, but I think the Air Force is doing a good job and doing a better job year by year. I don't claim any credit for this, because classification management is largely a matter of cooperation among a lot of people. Things don't get done by any one person. Here at the seminar, one of the most valuable things that will happen will be the interchange of ideas among yourselves, among all of us. Some improvements will result, and I hope that there will be a lot of that interchange. A little arithmetic shows that--at a time when we're all short on personnel in classification management--about four man years are being devoted to this seminar by your attendance, and the preparation for it. Or look at it another way: about a million dollars has been spent in travel, per diem salaries, and so forth. It doesn't matter whether it's my salary or Art's salary or the salary of any contractor. It all comes out of Government taxes, so I'm serious when I say the interchange of ideas should bring forth something productive.

In talking about improvements that have been made, I note again that they are matters of cooperation and I don't claim them all to be Air Force only. Some of the changes are major. Some are minor, but I think they're all representative.

First of all, in reviewing our Air Force guides, I see that the conversion to the fifteen-year declassification rule for scientific and technical material is appearing pretty much across the board. You have some guides that haven't been converted yet, but it's being adopted and put into effect in the guides as they're rewritten. It should be noted that the 15-year rule is not an idea that originated with the Air Force. It originated in Mr. Lieblich's office, in Mr. Van Cook's office.

We support it wholeheartedly.

Secondly, I think that the new security manager's course is probably the biggest single step forward that's been taken. There's been a real need for such a course. The idea originated with everybody, and if it's eventually a whopping success, it will be a credit to the people at the Defense Institute in Richmond as much as anybody. But I would note that on our own part, we went out of our way to help that school get off the ground by helping draft course outlines and by reviewing the course. And we took one step further: We looked across West Coast to East Coast to see who we thought was the best man to be an instructor in that course, and we recommended his selection. I hope the Institute finds him a happy choice.

As far as I know, only the Air Force has on its books one rule that is a step forward. That is a rule that permits any individual in the Air Force to come into departmental headquarters with no fear of being stopped by a commander along the line, and to be assured a reply, in any case where there is even the slightest allegation of classification to hide inefficiency or embarrassment.

Now, while we have had no such case reported, we feel the reporting procedure is particularly important. The problem in classification is not particularly that the Navy or the Air Force or the Army classify an operational plan. It is not particularly that we classify one piece of technical information. The major problems arise when and if people feel a classification is made to keep information from the public intentionally. Our rule as it implies states that any charge of that sort cannot be shortstopped, cannot be blocked from headquarters, and provides for the individual to correspond directly with us if he has not received acknowledgment.

Another point where I think the Air Force is doing well, and I think others are, too, is in the review of World War documents. Now, I'm told that the Air Force is well ahead of the schedule of completing this job by '75. We're moving ahead of others, and we're moving ahead of the pace.

If that's true, I think that Alan Thompson has a big share of the credit coming to him, because we sent him raw people over there. He sat them down and worked with them and provided them with administrative support and with the leadership to get something done on that job. A big job is being done.

Additionally, we moved outside of the archives and have the same kind of review going into our Air Force historical material, and I'm happy to say we've completed the World War II period and stand now between World War II and Korea.

Another point--one that I'm very happy with. Again, we're talking about old documents, and it has to do with the Library of Congress. It's a fair example of cooperation, I think.

There were sitting in the Library of Congress thousands of cubic feet of classified documents with no likelihood that they would ever be reviewed for declassification for two reasons.

One of them was that the Library of Congress was outside the Executive Branch and the second reason derived from the fact that the Library

had no declassification authority. This came to our attention in the Air Force and, admittedly, all we had was an idea.

We drafted up a proposal and wrote back to them, recommended they go in and ask for authority to apply the same guidelines used by the National Archives and to apply that not only for the Air Force, but DoD-wide also.

That action took us, I suppose, about one hour of our time. It took probably several score of hours to be staffed by Mr. Van Cook and others in his office, but it came out and the Library of Congress now has the authority and the guidelines and those documents that were frozen there before will be declassified.

I'd like to point to an area where I think the Air Force has done something very worthwhile. The rest of DoD has moved up ahead of the Government as a whole by moving from a thirty-year guideline to a 1950 declassification standard. Their policy says that all documents, with a few exceptions, 1950 and earlier, will be declassified. I'm happy to say that within the Air Force, for our own information only, we have similar guidance and have had it for some time. It extends through 1955, which simplifies the declassification a great deal.

In one particular area, we have made, I think, a very large achievement. I don't know how many of you have had occasion to see our nuclear weapons classification guide. It's been completely revised to bring it up-to-date in terms of the new Executive Order, and I believe that it will stand up in comparison with any guide throughout DoD or throughout the Government in terms of excellence as a classification guide. The particular reason I wanted to mention that here was to add a footnote for some of you.

A person that many of you know well retired just last month from the Air Force, and that's Ed Calvert. As an informational aside, for those of you who don't remember him, Ed was one of the originators of the Society, one of the people who sat down to talk over the idea, an original founder, an editor of the bulletin, and produced the finest series of professional bulletins in this area. He has retired and is back in Ohio. If any of you would like to get ahold of him, I can tell you how.

Some of the things that have been done in the Air Force that are noteworthy and the credit should go to activities below Headquarters level. In our Space and Missile Systems Organization at L.A.,

we have an exceptionally fine program for presenting the guidance to the man who has the authority to make exceptions to the GDS, and for processing this material through so that proper approval is received. I'm not going to discuss it in detail, because Mr. Klein will talk to you about it later, but I note that OSD has seen fit to point to it as an example which we can use elsewhere in the Air Force.

I'm sure that the Air Force was ahead of all other agencies in any part of the Government in establishing a desired objective of stating a topic-by-topic declassification date, rather than the mere entry of GDS or XGDS in classification guides. We haven't reached a point where that's done in all guides, but the guides are coming in in large numbers with Topics identified for downgrading to 1 such-and-such, information, secret, confidential, and unclassified with the year shown for each action. You'll find that a large amount of the work on that, in some of the best guides, is coming out of our Aeronautic Systems Division, where Mr. Gates is in charge as far as classification is concerned.

One more item: earlier, Mr. Liebling mentioned the authority of the Assistant Secretary of Defense to declassify documents. In our initial implementation, we gave to our Air Force Office of Information the full authority to declassify after completion of their security review, and this has sped up the process many times.

It doesn't mean they can overrule the Air Force, but it does mean the results of their review are authority enough without going back to anyone else.

As a general statement, and I hope that others here would support us (I am thinking primarily of AF), I believe that in any case where there's been a proposal for liberalization and broader declassification standards, the Air Force has, without exception, supported the proposal. Now, there'll come a time, I'm sure, when we'll be on the other side, but I believe our performance to date will show that in general we are pushing for broader declassification guidelines and earlier dates.

As a last point I'd like to mention again that from all of this, I don't claim a superlative job. There is always room for improvement. We think we're doing a good job, and we think we're improving.

I'd like also to get back to my initial point about the hope there will be an interchange of

ideas here. I know Fred Daigle and I met down at Richmond where he was kind enough to come and help in the critique of the security course. He gave me a problem of his, and by the time I'd been back in Washington a few days, I think we'd solved it. Jim Buckland was there and he raised a question to me. We were able, I believe, to give a satisfactory answer. I hope that the Society here will try to solve problems and make real progress for all of the Government community by turning this four man years and million dollars into productive discussion back and forth amongst yourselves.

Thank you.

QUESTIONS AND ANSWERS

MR. JERNIGAN: John Jernigan, General Electric, Philadelphia. If we question the classification on some specific light and we don't receive an answer or satisfactory answer within thirty days, do we come back directly to him? Does this apply to you, Frank, and to you, Larry, also?

MR. LARSEN: Be our guest.

MR. MYERS: Absolutely. We expect all contractors to deal within the contracting office, but if you're not getting satisfactory replies, why, let us know.

MR. VAN COOK: Yes, sir.

MR. HOYLE: My name is Jim Hoyle. I work for the Lance Project Office, Missile Command, Alabama.

I'd like to make a couple of statements, if I may, and address my first remark to Col. Grimes. I can sympathize with you, Colonel, in your deluge of screening and sanitation. But, getting back to contract security specification, more commonly referred to as DD 254; if these are properly filled out, especially front and face, in the lower left-hand block is a space to be filled in with the name of the action officer for the project, or what have you, who are purchasing the hardware.

Now, at the Missile Command, we've had some good guys, and so forth, and most of these are properly filled in with the name of the individuals to be contacted, with a telephone number in case you can't get a satisfactory answer from the contracting officer.

So as the action officer for Lance, I get many different phone calls from time to time and if I'm not able to give a correct answer quickly, I can at least tell the people where to go.

I get questions from time to time, of course, from contractors other than for Lance, even, and I'm able to direct those people to the action officer for the nearest project that they require assistance from.

Secondly, I'd like to get back to the information that we at the, I believe, lower grass roots level need from time to time. It took us a year working, pleading, cajoling, whatever word you'd like to use, to get some direction at high level.

It came back in the form of a twist from DoD through State Department, down through the line on the classification of the foreign military sales information.

Many of you contractors, I'm sure, have gotten into this area, but we were groping for facts. Provided with the facts, we can operate satisfactorily and give good direction; but that's one of my biggest problems is getting accurate information in order to prepare a good decision on the security classification guide, so I'd like to put that in the form of a suggestion, maybe, to DoD and let it filter on down that they look into supplying certain information along this line to the various people in the various weapons systems.

I say from time to time, as the need arises that now systems are being developed or as the international situation changes, and so forth. It would be very, very helpful to us.

MR. NILES: Bob Niles, DNA.

In the last few years, lots of people from classification have protected somebody from embarrassment or administrative oversight. Do you have any specific knowledge of a DoD document that was classified to protect any individual from embarrassment or oversight, and I mean the document discovered by anybody to include the executor, legislator, for any branch of the Government?

MR. VAN COOK: Do I have any personal knowledge of any such document?

MR. NILES: Yes, sir.

MR. VAN COOK: That was classified to--

MR. NILES: Hide embarrassment? Yes, sir.

MR. VAN COOK: The answer to that is no, I don't have any and I'll ask my colleagues on the panel if they have any knowledge? They don't have any knowledge of any such document, either.

MR. MARGAROLE: We have a lot of old documents. My engineering friends tell me we can't throw them away, because they contain a lot of good systems information. However, since the program officers way back when disbanded, we do not know whom to write, per se, for classification guidance, and would you enlighten us perhaps to this subject?

MR. VAN COOK: I think I can. You contact the USER Agency under whose contract you are operating at the current time, and then there is a provision I think you'll find in the Industrial Security Manual that says you can take other routes if they can't give you a judgment.

MR. MYERS: Art, can I make a short comment on that? From some of you, we've had requests of this sort and I think they have sometimes been delayed by your taking what you think is a direct route and sending them straight in. Some of you people from DCAS can stop me if I'm wrong, but I believe that the DCASR would always be glad to assist in telling who the successor agency is. The contractor should know who his contractor was and when there's been a reorganization. I believe that the DCASR would go off and get an answer to that question so the contractor could go to the right office in the first instance.

Anyone from DSA care to comment on that?

MR. GREEN: Office of the Chief of Industrial Security, Defense Contract Administration Services.

Yes, we could trace it back just as you can trace it back through the military departments. It could be traced back through contracting channels.

LT. COL. GRIMES: In the Army, if you have a classified document and you have absolutely no idea who to send it to, the proper place to send it to is the Army Adjutant General, Department of the Army. He's required to keep all statistical data. He is also required to keep what we call a record copy. He's responsible for the archive information material for the Army. He will get it to the appropriate agency that is presently handling that particular project or who has proponentcy for it. So if you're going to deal with the Army, deal directly with the Adjutant General. It's the fastest way of doing it and it stays in the right track.

MR. LARSEN: May I make a comment about the Navy, Art?

MR. VAN COOK: Go ahead.

MR. LARSEN: If you're not able to identify the procurement activity, send it to the Chief of Naval Material who will either locate the material or send it to my office.

MR. MYERS: While we're kicking that around, Art, the ISM gives you an address in every instance for each agency to whom you can send it. My only point is that your DCASR man is in your area frequently. Frequently, he can answer the question out of hand for you through his own familiarity. If you do that, you may save yourself a lot of time.

MR. VAN COOK: Thank you. Any further questions?

MR. GREEN: A two-shot question for Colonel Grimes. Are you charging this individual the price per page for the reproduction of those documents?

LT. GRIMES: Five cents.

MR. GREEN: Five cents?

LT. COL. GRIMES: Five cents a page.

MR. GREEN: My second question is what office in the Army makes a final decision as to what the classification is?

LT. COL. GRIMES: Okay, I'm going to take you through it. First, you have the initial request for the document, right?

MR. GREEN: No. I'm sorry--

LT. COL. GRIMES: Well, I think I have to go that route, because you wouldn't understand it, otherwise, okay? It comes to TAGO or the Adjutant General. He forwards it to the proponent agency and they say the document is classified. They have the authority to say the document is classified.

Now, if the document is less than ten years of age, it would go to the final approving authority, to the Secretary of the Army and that would be it. If he says "Yes, it's still classified," then there would be no appeal. Normally TAGO will write back to the gentleman who asks the question or asks for the document and they'll tell him that based upon the proponent's suggestion or evaluation of the document, it remains classified, and they'll either tell him that he has a right to appeal to the Secretary of the Army or to the Army Classification Review Committee, depending on the age of the document.

MR. GREEN: I think I make myself clear, but I'll see you afterwards.

MR. RICHARDSON: Texas Instruments.

Art, I heard a little bit about the fifteen-year rule. I have several documents that are declassified in two thousand and something, which is thirty years. Now, does this fifteen-year rule that we've heard about overrule these decisions, and when we get these 254's in so identifying, can we avoid marking them down and having to remark them when this becomes a fact?

MR. VAN COOK: I would say no to that, Dean. The DD Form 254 is the contractor's guidance. If a DD Form 254 shows thirty years rather than fifteen, I think that ought to be brought to the attention of the USER Agency people to have that guidance changed. The guidance will, in fact, be changed as it comes up for review, and these are some of the things that are happening. I mentioned the thirty-three hundred guides to include DD Form 254's, which have been revised to cause earlier downgrading or declassification. I think you have to go through the business of getting the guidance changed, and the way to do it is if you want it done earlier than the annual review is to bring it to someone's attention, but I'm not telling you to overrule whatever guidance you may have from the USER Agency, on the basis of the rule.

LT. COL. GRIMES: There is an exception to that rule. You have to remember now it's DoD material, so don't apply that rule and say it's ironclad, because, in some instances, there may be cases where the organization that's giving you the contract, the contracting official is using information that isn't completely under the purview of Department of Defense. It could be coming out of the White House or from some other source that data has been extracted from, and these other sources have, in fact, said declassification in thirty years, and so there is a stipulation in 5200.1-R of what you would use in there, so the fifteen year rule wouldn't apply in all cases.

MR. RICHARDSON: There apparently is a misconception then in the minds of a large number of the people that write these 254's in the procurement agency. We've gone back and questioned some of these and they've said, "Our guidance is in accordance with 11652, which provides for an automatic declassification thirty years from the date of issuance," and I'm wondering if the agencies are waiting for the DA or another instruction to tell them to change their guidance to a declassification after fifteen years.

MR. VAN COOK: No, the change has been reflected in DoD regulation 5200.1-R. That regulation is self-implemented, so that everybody has that now. The regulation was dated November, 1973. It came out of the Government Printing Office and was published in a Federal register in March of this year. The information is there and they have it in regulations, so I would attribute the condition to a misunderstanding perhaps, Dean, but these are the things, of course, we're trying to get straightened out and particularly in this program for review of security classification guidance to bring it up to speed, and in those cases where it comes to your attention, we again invite the challenge.

MR. WESLEY: Roy Wesley, Grumman Aerospace, and in connection with Dean's statement, what about the DD 254 where you have declassifying on it indefinite; what about the other side of the coin?

MR. MYERS: I suppose that's an Air Force 254. There are a large number of those. Until the revision that came out a few months ago, Air Force was using the term indefinite and we have put the word out banning "indefinite" and I've seen many, many changes coming in. I think that each of the services was using a different notation prior to that time. Where you see it, it's outdated and should be picked up in the first review. We have not required people to go out on an interim basis, but many of them have.

If you need a change before then, ask for it.

MR. LARSEN: Is it not true that this is of primary concern to you on subcontracts?

MR. WESLEY: Yes, sir, absolutely.

MR. LARSEN: As far as the Navy is concerned, you can ignore the indefinite and use that classification guide and substitute thirty years. Go right ahead, but let us know.

LT. COL. GRIMES: The term the Army used was probably "cannot be determined."

MR. MYERS: Don't accept wrong guidance. Go right back to the issuing office. It's not embarrassing. You're not questioning the individual. If you have a question request clarification, and reference 5200.1-R or the ISM.

MR. VAN COOK: The regulation now prescribes that in all cases, dates, in fact, will be used. Please bear in mind that this is only going to

be in the instances where the Department of Defense exercises exclusive final classification jurisdiction over the information involved.

If the information is foreign originated, for example, the notation will show that the material will be declassified upon notification of originator.

MR. RICHARDSON: Art, a lot of my questions, of course, are predicated on a problem that faces us as well as many other industry people and that is the overhead cost of doing business.

That's one of the reasons that I was sort of hoping that you would give me an affirmative answer, but as your predecessor mentioned to me one time before, he said, "Dean, you're over-ruled."

Art, I'm not going to say that.

The problem facing us when we start putting marks and identifying things on such things as drawing--I'm talking from a hardware development standpoint or even from paper to paper--but when you start changing drawings and things like this, it becomes extremely expensive, so I was hoping there would become an automatic method of saying that's not right, we're going to the fifteen-year rule.

I understand what you're saying.

The question I would like to ask now also reflects on a lot of our problems and on a lot of our budgets. We're all faced with revising our standard policies and procedures and this, in my case, is going to be somewhat expensive, and I think Western Electric at one time said it cost them a thousand dollars a page to revise their SCP, but the point is we would like to hear from you, if possible, to give us some idea of things that are being changed and probably being changed in ISL's perhaps during the next few months, such things as elimination of the excluded category, for example, or some of the other changes in the kinds of things that we have to educate our people on and worry about buying stamps for and worrying about putting on drawings and things of this nature that are terribly expensive to remove and change.

MR. VAN COOK: I understand. We don't anticipate any major changes. I can't give you an immediate prognosis on what's going to happen from here on in. These are some of the things that our experience of over a year of working with the Order and with regulations which we found really required change to be responsive to our needs.

They're evolutionary changes and they come about after due consideration of the things you're talking about. The program needs to work, and we're hell bent on making it work.

I understand what you're saying about costs coming up as the result of an action which is initiated by the Government, but I believe that when a contractor puts in for a bid in the normal course of business, he has the Industrial Security Manual and he can anticipate that there will be certain information that he starts off with at a secret level, perhaps, which may be downgraded or declassified at some future time.

I mean, he understands that, and so in figuring your overhead for any contract or bid, then I think these things you must take into consideration, and it's just the cost that is associated with everyday business. If you go into it with that understanding of what is in the ISM, and that there is a progressive downgrading and declassification system in effect and you're going to have to cope with it. I think it's a "plan-ahead" operation so that you have to allow for it from the very beginning. That's just the way people do business.

They have to anticipate these things. To try and say that next week we're going to do something that will make the program even more progressive, I can't anticipate that at the moment, but if, as we go along, we find that we do have to make change to make the program a more progressive one, we'll just have to do that. It's just a matter of practical approach that people have to go into it with their eyes wide open.

Jim.

MR. BUCKLAND: I think, Art, that what Dean is saying--something that we discussed before last March--is this: We're talking about this fifteen-year business. I think that in the last month, I probably got in six or eight new 254's--either revisions or originals. None of them have the 15-year declassification date. All's still indefinite. Now, I know that that's wrong. I have to get it changed, but, in the meantime, I'm generating documents.

As soon as I get that directive, which may take anywhere from one month to six months, depending on who I'm dealing with, I theoretically should go back and change those documents.

The kind of change that I think Dean is talking about, and I think we've talked about it before, and I think you agree that if we have to change

our markings on our documents be a use of initial erroneous guidance, that the contractor has the right if he so desires to cost the impact to the Government for those changes providing he was the contractor which followed the specific written instructions.

I don't think it would cost impact, but I think you should allow for that in that provision.

MR. VAN COOK: Well, I think you have to take a practical approach. We discussed this when you were in New England.

I think, Jim, there are going to be these changes as reflected in your revised guides. We don't expect that the contractor is going to reach back and modify every document that has been created back there based on that change.

We think that when a document is withdrawn from file or storage for any purpose, that's time enough to make that change.

I think that the DCASR inspectors should recognize that. We're certainly pushing for it. We have some regional representatives here and they should really understand that when the Government comes out with a change to guidance, that it's not expected that the contractor will reach back and mark every document he's created from the beginning of time to right now.

We think the time to do that is when the document is withdrawn from the file storage for any purpose, and I think the members of the panel will agree with that.

It's just going to be a practical approach and we would hope that the Defense Contract Administration Services Region people will take that approach as well. Any further questions?

MR. COOK: I'd like to make a comment, Art. I'm R. J. Cook from General Dynamics and Convair.

We have a problem with the DCASR noting this each time he comes in and he writes us up in a deficiency statement.

We can't keep up with the changes, so we would appreciate any advance info we can get.

MR. VAN COOK: Thank you very much. We have in the audience today Mr. Green, who is representing the office of--(laughter)--who is representing the office of the Chief of the Industrial Security at DCAS and we've discussed this matter before and I think Bob is understanding of it, and if this

kind of guidance is needed, I would hope that you'd take a look at it, Bob.

MR. GREEN: At this time, Art, I'll only say that we have a meeting tomorrow night with the representatives of the region here, and I hear what's being said today.

MR. SHARE: My name is Don Share. We've all addressed a lot of different problems here this afternoon and I notice George has put out the good word that we're about fifteen minutes overtime.

It's been an excellent exchange of information here this afternoon, but the people who are most concerned with what we're doing are not represented here. As an intelligence officer, I look at myself as the enemy representative on my commander's staff, so I would like to speak to you as a Soviet intelligence officer now.

When you start releasing this plethora of technical information, please let us know. We'll have to staff about another two hundred thousand people to read all the technical data you'll supply us.

There's not one word in 11652 that I can ascertain that says please don't underclassify, but when we're looking at this stuff, I sure hope we'll look at it with that in mind as well as trying to comply with the Presidential intent to get a lot of this stuff out of our files, dump the stuff we don't need, keep the stuff we do need, but for God's sake, let's don't let it float down the river. (Applause.)

MR. VAN COOK: Was there a question over here? Yes.

MR. HIMMELHEBER: J. Himmelheber, from Hitco.

I'd like to suggest that it is possible upon receiving classification guidance which contained an erroneous entry such as an indefinite date, I might be tempted not to date and to report that fact to the contracting agency and that way I wouldn't have to remark. I'd just have to initial a remark, just leave it blank.

MR. VAN COOK: The rules are out there and it takes a while for things to happen, as you know, but they are happening.

Well, I was just going to summarize, but the Chairman has exercised his option to throw one more question at us. Fine.

MR. CHELIUS: DoD Regulation 5100.R with respect to the general declassification schedule provided that the USER Agency could exempt that material within one year. You have now promulgated this regulation as far as downgrading Group 3 information in accordance with the old schedule. No such provision was made in the regulation for user agencies to exempt formerly Group 3 material.

During the period that the old regulation was in effect and the Group 3 downgrade declassification was in effect, many guides were revised to show that material to be exempt. What is the position of your office with respect to that material?

MR. VAN COOK: We think that upon review, whether the items of information in a security classification guide or in a contract security classification specification started out in Group 3 or GDS or ADS, for that matter, upon review, the original classification authority could opt to remove it from that category and put it into exemption category.

However, he can only do this if he does it at a time before the automatic declassification takes place. Once that has happened, forget it.

Well, you've heard from the panel. We've enjoyed the exchange. One of the recommendations of the Society was to consolidate all our security classification guides in one place.

You heard that the Navy has already started to computerize its guides. We think that we will be able to do that with all the departments and agencies and put the consolidated listing in the Defense Documentation Center or some centrally located place. We are looking at that. The guy who let that one slip stands right here. I just haven't had the opportunity with the activities that are going on in our own office and with the Congress and with other things during the past months to get at this program.

I promise this audience that I will, within a very short period of time, get those guides together and collect it in one place for all to use, and we will be working on it just as soon as I get back from here.

PANEL: LIBRARY COUNCIL LOOKS AT MAINTENANCE OF
ESSENTIAL CLASSIFIED TECHNICAL INFORMATION
MRS. JOE ANN CLIFTON, Moderator
Manager, Technical Library, Litton Industries

MR. H. W. JONES, Panelist
Manager, Library Services, Northrop Corporation

MR. B. W. CAMPBELL, Panelist
Supervisor, Company Technical Document Center
Hughes Aircraft Company

MR. JOHN BERRY, Panelist
Research & Development Liaison Officer
Department of Defense (Retired)

MAJOR HAROLD G. HOCK, Panelist
Scientific and Technical Liaison Division
Headquarters, U. S. Air Force Systems Command
Andrews AFB

MR. MYER B. KAHN, Panelist
Chief, Accession Division
Defense Documentation Center
Defense Supply Agency, Cameron Station

PRESENTATION BY MRS. CLIFTON

One of the biggest problems which you as members of this Society face is whether to classify a project and its resultant documentation, and if to classify, when to classify it and its material.

Now, another element of this problem is the maintenance of the classified information until its declassification. What, where and for how long, as well as what to release is a vital concern to those of us who are responsible for disseminating information.

The motivation behind our choices is based on getting the needed information to our users in the specified time, at the smallest cost both to the Government and to our companies.

Hence, we information specialists, whether we be known as librarians, documentalists, analysts, archivists or managers, face a dilemma today.

Current DoD retention regulations have not allowed us to make the correct choices in many instances. Therefore, we have found and with more and more frequency, the deplorable situation of the wheel being redesigned because the necessary documentation was not there when it was needed. In some instances, companies have originated reports, destroyed the documents after they have sent the original to DDC, and found at a later time that they again needed a solution to the same problem. Some of our engineers who couldn't quite remember how they had solved the original problem, tried to get a copy of the report back, found that we didn't have a current need-to-know in that particular area and were unable to get back our own report. As you all know, that can be just a wee bit frustrating.

Because this retention problem was common to so many companies, it was chosen as a project by the Los Angeles Regional Technical Information Users Council, called LARTIC for short, for obvious reasons.

This was a council started in 1970, whose purpose was to study and attempt to stimulate, improvement in all the Government services.

This included giving commendation for excellence in service when it was indicated and we have done this to several agencies.

Members of the council are in companies that are located from Santa Barbara down through the San Diego area.

After we had done the research on each of our selected projects, we published a comprehensive report and then send copies to everyone; first of all, to the agency affected, then we send it to a Congressman, any committee that's in any way involved in policy-making, especially those impacting on the budget of the agency concerned.

We have gotten excellent results.

The retention project that we're going to be discussing today will be included in our forthcoming LARTIC Report No. 2, which will be published in September and will be available from NTIS.

Two of our council members, Bill Jones and Bill Campbell, are here to discuss the council's views on recommendations. They are not here speaking for their companies, but on behalf of the council. In addition to Mr. Jones and Mr. Campbell, we have three other gentlemen on the panel, Major Harold Hock, who is director of the Air Force Scientific and Technical Information program, Scientific and Technical Liaison, Headquarters, U. S. Air Force Systems Command, and he's in charge of the potential contractor's program which was previously the TOD Program.

He will be speaking to us about the new Air Force potential contractor's program and its plan for retention authority for those in the program.

Another speaker will be Myer Kahn, Chief, Accession Division of the Defense Documentation Center, who will speak on the retention problem as it affects DDC and its users.

Our fifth member of the panel is John Berry, recently retired from the Department of Defense as Research and Development Liaison Officer, and who had the prime responsibility of liaison work between contractors and all echelons of the Department of Defense.

He interphased with other Federal agencies in the fields of industrial security, contract management, and production of technical information.

John has seen the problems from both sides of the fence, and we thought perhaps he would be able to express a more objective viewpoint with perhaps a recommendation of his own from his years of experience.

Now, the order of the speakers as they appear in the program is not how they're going to appear this morning.

I will briefly introduce each speaker before his presentation. We will have the question and answer period after the presentations have been made.

With that, I'd like to introduce our first speaker, who is N. W. Jones, better known as Bill Jones, who is the Manager of Library Services at Northrop Corporation, and who is one of the members of our council.

PRESENTATION BY MR. JONES

To begin with, I'd like to set the stage for this presentation by making clear what we mean by a library or information center, which is the kind of organization those of us on the Council represent. We're talking about contractor libraries, large and small, which function as the central agency in the acquisition, receipt, storage, dissemination, and retention of technical information, both classified and unclassified, in support of government business. We're also talking about basic procedures which must be established to control and retrieve this material, including requirements of the ISM, such as accountability and retention authority.

Basic criteria for use of classified information by an individual are clearance and need-to-know. Further, we assume that each document at the moment it is acquired by the library has a retention authority based on a need-to-know, else it could not have been acquired in the first place. Obviously, then, the document in use would normally have to have a legitimate retention authority. Consequently, what we are really concerned about--what constitutes in our minds the real problem area--are those documents in the collection which at any given time are not in use, and whose retention authority may be questioned. This, I believe, is the crux of what we will be talking about here today, and it relates specifically to both direct and indirect costs of doing business.

So let's examine this cost of doing business as it relates to classified material, with the ultimate objective of our discussion, hopefully, to find possible solutions which may lead to a

reduction of these costs and still retain optimum useability of the technical information available within reasonable protective constraints set up by the government.

Costs of the library function include, first, the acquisition process. A document may be acquired in several ways, the most common of which are (1) receipt on automatic distribution from the originating agency; (2) direct request to originator, and (3) direct request to secondary distribution agency, such as DDC. These are relatively routine methods, except for documents in the DDC collection whose distribution has been limited by the originating and/or contracting agency. These are known as "L" documents, and unfortunately a very large percentage of them make up the DDC holdings. This limitation not only requires additional paper work in the ordering process, but also delays receipt anywhere from one to several months. This is costly not only because of additional handling requirements, but more importantly, from excessive delays which may well be critical if the project involved is a short-fuse proposal or a one-year contract. The consensus from the Library community is that the imposition of distribution limitations on documents (other than security classification) seems to occur much too frequently and with far too little apparent consideration for the ultimate potential user. Added to this cost, of course, are the "hard" dollars spent in the actual purchase of each of those documents.

The second significant cost is the indexing of the library collection or data base. A document, or the information it contains, is useless if there is no access to it, or if it cannot be easily retrieved. Therefore, its real usefulness, if it has any intrinsic value for the user agency, is directly related to its points of access, or how easy it may be to find it from whatever description you may have of it. To provide access or retrieval capability the library must go through the expensive process of indexing. In most cases in a library, this is exemplified by the card catalog, where the existence of information in a document, or the document itself, can be traced in several ways--by one or more subject terms, one or more personal authors, one or more corporate sources or authors (commercial and/or government), one or more report numbers, and even one or more titles.

Finally, because the material is classified in the first place, there is the very significant cost imposed by security regulations involving special handling, controls for accountability, storage, transfer, destruction, etc.

The foregoing are essential and accepted costs of doing the kind of business we all are involved in, and good managers try to hold them to a minimum commensurate with doing the best possible job. But some costs which seem to be beyond our control and are most frustrating and agonizing are related to the requirements of retention authority. Here, we have to go through the expensive process of renewing or obtaining a retention authority for documents in our collection which still may be pertinent to our general capability. Or else go through another expensive process of getting rid of them, and then at some later date, be asked to re-acquire the same material for some other specific need. Here, the original activities of acquisition, indexing, etc. have to be undone when we get rid of them and then redone when we re-acquire them, which in effect is tripling the original cost of the function. Not only, that, there is the intangible cost of delay in obtaining the material, or the possibility of having to "reinvent the wheel" because the material is not readily at hand. We feel strongly that these are largely wasteful and unnecessary costs and could and should be eliminated. The rationale for our feeling goes something like this:

The objective of the contractor librarian is to maintain a useful, manageable, relevant file for his users. Non-relevant material will not only increase his maintenance costs, but also produce a larger percentage of false-drops, or, non-useable material in response to a user's requirements; this will add to the user's cost also. Therefore, the librarian will not want to retain non-relevant material--or in other words, he will get rid of material when it no longer can serve his needs--or when he, in effect, no longer has a "retention authority." Since the contractor librarian will make every effort to keep his collection realistic, efficient, and dynamic by eliminating "dead wood," he shouldn't have to go thru an expensive and redundant process to re-justify retention of documents already in his collection.

A contractor with a DoD facility clearance based on contracts, grants, or a capability to provide products or potential products for the DoD should be able to retain any supporting documents for as long as this relationship with the DoD exists--not just as long as a specific contract exists. Therefore, rather than retention being based on specific contract coverage, a general retention authority should apply, based on the contractor's DoD approved capability or "Area of Competence," with the contractor being the best judge of what will support his efforts in behalf of the government, instead of the other way around.

Earlier, in describing acquisition of material, I mentioned receipt of documents on automatic distribution. This of course, costs the recipient nothing, insofar as acquisition is concerned. But I'd like to pursue this point further now and show how it does have a direct and rather significant bearing on the cost of handling classified material--and one which we feel can definitely be improved upon and reduce costs.

To set the stage for this, let me review briefly a bit of history. The post-WW II information explosion, brought about by the \$ billions spent on R&D in all areas of DoD weapons systems and related science and technology, generated hundreds of thousands of reports, including a high percentage of classified. Distribution lists were created in order to disseminate this valuable information to all who had a need-to-know (and perhaps many who didn't). One rather famous list was the "Guided Missile Tech Info Dist List." All contractors who were doing any work in this area--and some which weren't--were on this list and automatically received reports as they were generated by any of the others. All of us got each others' reports, whether we really wanted them--or more importantly, really needed them--or not. This sort of thing proliferated the dissemination of classified documents for years--before "retention authority" became a buzz word. But now, of course, such "indiscriminate" dissemination is a thing of the past. Or is it?

This method of dissemination may be a bad habit that some agencies can't seem to break--or else it just hasn't occurred to anyone to try to find a better way.

Some suggestions:

1. Reduce primary distribution to a "hardcore" few. Let the secondary distribution agencies--such as DDC--handle the dissemination of classified reports based on specific need-to-know.
2. Send only to one central spot (library) in any organization--let this central control handle further dissemination within the agency/company.
3. Do not send to individuals but mention them if its important for direct internal contact.
4. Audit each list at least annually.

5. Send only unclassified announcement of publication--with abstract--and info concerning its acquisition.

We feel such actions as these would cut costs dramatically in the handling of classified material, but could only be effective if the appropriate government agencies are able to communicate at the right levels.

In a nut shell, then, I've tried to get across two important points which could lead to reductions in the cost of handling classified material:

1. Base retention authority on sponsored and authorized capability or Area of Competence, rather than specific contracts.
2. Eliminate or drastically reduce the automatic, primary distribution of classified documents.

PRESENTATION BY MR. CAMPBELL: Consequences of Full Compliance with the Present Law (i.e., without questioning)

Possible consequences include:

1. Destruction of basic reference documents

A reference book, according to Webster's, is "A book (as a dictionary, encyclopedia, atlas) intended primarily for consultation rather than for consecutive reading." To the librarian, reference books include continuation publications such as symposia proceedings, classified periodicals, indexes, bibliographies, etc. which form the basic research materials that are essential to the library's function, and which are often irreplaceable.

Premature destruction of such materials is costly to the customer. Because of time restraints written into proposals or contracts, engineers frequently cannot wait for the library to reacquire such materials, if available, and they proceed to reinvent the wheel. The Government pays for research that has already been accomplished and paid for elsewhere.

2. Incomplete or inefficient usage of government furnished bibliographies

Use of retrospective computer searches of NASA's and DDC's collections results in valuable bibliographies. These are rendered significantly less useful when the documents cited are not available immediately because of reasons outlined in "1" above.

3. Reacquisition of destroyed documents

Destroyed documents have to be reordered as required. Current costs are \$3.00 and up for full-sized copy, and \$1.45 and up for microfiche versions. To obtain the documents staff time is required from the requester, the library, the mailroom, classified document control, and others. To be maximally usable, the document may have to be cataloged again, at a cost which traditionally costs as much money, or more, than the original cost of purchasing the document. All of this eventually increases the cost to the customer (the Government).

4. Hindered response to contracts and requests for proposals

Many classified document requests are for use on short-term contracts, or to answer requests for proposals, with very little time to acquire documents of possible value. In order to acquire documents for use on a contract, one contractor has to wait for the DD 254 authorizing use of the Defense Documentation Center. Then, Form 1540 to register the contract with DDC has to be completed. Three to four months delay before we can obtain documents on a contract is usual rather than exceptional. Proposals can not be registered at all, and customer furnished data are frequently not received on time.

5. Under-utilization of government funded research

Technical contents of proposals not leading to contract awards should be preserved for adaption to other efforts. Enforced premature destruction of such data prevents another potential customer from receiving the benefits of previous research.

Recommendations

The Los Angeles Regional Technical Information Users Council recommends that the Department of Defense consider the following:

1. Technical library/information center central repository

Recognize the technical library/information center as the central repository for classified reports and information necessary to a company's successful performance of contracts.

2. Librarian/information specialist

Recognize the librarian/information specialist as qualified to determine which documents are appropriate to acquire and retain, based on DDC Form 1540 and DoD Form 1630.

3. Enlarge the concept of retaining reference material

Industrial Security Letter 70L-6, 18 November 1970, says of DoD's Technical Abstract Bulletin (TAB): "The Defense Documentation Center (DDC) furnishes classified TABs to contractors who have been certified and registered for receipt of selected scientific and technical information. The TAB is furnished so that eligible contractors may have subject matter abstracts of documentation which is available and usable on one or more classified contracts. Accordingly, the TAB may be retained by a contractor as long as his facility has a valid registration (DD Form 1540) on file at DDC..."

This concept should be enlarged to include other basic works such as bibliographies, Classified Scientific and Technical Aerospace Reports (CSTAR), the Journal of Defense Research, Infrared Information Symposia proceedings, etc.

Companies with demonstrated competence in a field should have retention for a reasonable period of time, say eight years to match the new General Declassification Schedule. At the end of a stated period, retention renewal could be applied for.

4. Allow retention of all classified documents that cost money, or eliminate charges for them

Companies must pay a handling charge to obtain classified documents formerly furnished free of charge; companies should have the right to retain these documents as necessary, based on current certification of Fields-of-Interest. If this is unacceptable, we recommend that charges for classified documents be eliminated.

5. Recognize Form 1630 as a basis for document retention

DoD Form 1630, "Research and Development Capability Index, Scientific and Technological Fields of Interest," should be a legitimate

basis for retention by subject areas, rather than by individual contracts. The Government awards money for IR&D effort based on the 1630, so it is not logical to impede our performance of tasks the Government is interested in.

AND/OR

6. Recognize subject areas of contracts registered with the Defense Documentation Center as a basis for document retention

Precedent exists for this in that DDC's Automatic Distribution of Documents program was based on a compilation of registered contracts.

7. Recognize the archival function of the technical library/information center to retain company-generated documents

It has been the experience of most contractors that after destruction of company generated classified material, it has subsequently become necessary to reconstruct as well as possible, from memory, material contained in those documents. The Government should recognize the archival function that libraries are frequently charged with, and allow them to keep internally generated documents on that basis; or at least, contractors should be allowed to obtain their own documents from DDC or NASA without expensive procedures.

8. Retention of proposals

Allow retention of proposals, together with documents acquired or generated in the process, in order to respond promptly and effectively to future Government needs.

9. Improved Communication

Improve intergovernmental communication and instructions so that DCASR agents within a region, and between regions, interpret regulations uniformly. It has been the Council's experience that uneven interpretations have, on occasion, worked to the detriment of one contractor compared with another.

In summation, we submit that in today's economy, we do not store documents without due consideration of their possible need in future programs. Documents require space and cost money, and libraries are chronically short of both. We expect to be responsible for the documents we have; we merely ask that documents be made easier

to retain so we can perform work more efficiently for our customer, the Government.

PRESENTATION BY MR. BERRY

I have been referred to as the "Crusader of the Technical Information Program" because of my continual concern for the improvement of controlling, classifying, releasing and accounting for the billions of dollars worth of technical information that should be readily available to the industrial community. For the past 32 years, I've been trying to improve the system and at the same time work within the framework of a dynamically changing but poorly constructed information system at all levels of government and industry.

Today, after 32 years of government employment, I am a retired citizen and will pass on to you some of the observations about the frustrations that confront your corporate libraries and those of us trying to support the technical engineers' and scientists' information requirements, while operating within system restraints, compounded by a fantastic flood of technology that has been labeled the "information explosion."

About ten years ago, as a civil service worker, I was assigned to what was then called the DCAS (Deputy Commander of Aerospace Systems), Technical Data Center of the Air Force. My responsibilities were to determine, with the System Program Offices (SPO), what documents were to go into the Armed Services Technical Information Agency (ASTIA) which is now Defense Documentation Center (DDC). Documents that didn't go to ASTIA at that time remained within the Air Force Technical Data Center and were tightly controlled. But my next job was with DDC and I became a liaison officer, responsible for traveling in all fifty states and some foreign countries, to teach contractors and military how to utilize the services of DDC.

It was my job to get together with the military and civilian industrial security officers and tell them what was wrong, get together with and lecture the Procurement Contracting Officers (PCO) and administrative contracting officers on problems. It was my further responsibility to get together with the SPO and project officer at the lab level and work with the librarians to try and resolve the lack of coordination between originator and user of the documents. Most of the engineers working in industry do not understand the problems facing their librarian. He or she has to acquire a document that is controlled beyond requirements or buried in some SPO's file cabinet.

Let me tell you a true story about an engineer who wrote to us at DDC; he was trying to get direct access to classified information from DDC. I visited the engineer at his company, got together with his boss and we walked to the library. I said,

"Did you ever hear of your company library?" He said,

"No."

He had to pass it every day going to the cafeteria, and the librarian rode in his car pool! This is a typical example of what I am trying to emphasize about lack of communication.

The PCO's have to learn what their responsibilities are in relation to DDC. The inspectors in the industrial security office are justly concerned with the idea of eliminating unnecessary documents from the contractors holdings. They don't want the contractors accumulating large holdings of documents that are not being used. But, at times, the lack of communication between the PCO, SPO, Industrial Security Inspector and DDC results in a state of confusion for the contractor.

For example, we had a PCO in the Army tell a contractor to destroy five hundred secret documents. The contractor complied, and about a week later the contractor was requesting from DDC the same 500 documents, approved by a new PCO. The company had to pay for those 500 documents all over again. Situations like this put a drain on our economy. So who is kidding who? We've got problems.

Another problem area is declassification of documents. In my job at DDC I saw more documents with the exempt stamp than with the downgrading stamp. Do you know what the problem is going to be in the next three to five years? Trying to find the lieutenant who put the exempt statement on the document, so that it can be released to the contractors.

DDC is suggested as the center within the DoD with responsibility for distribution of DoD funded reports. It will never happen. Why? We have too many project officers and SPO's that have documents buried in their safes. Through a search at DDC, I found that three thousand organizations never contributed a document to DDC, yet they had DoD contracts.

To portray the problems, frustrations and loss of time and money, let's take a typical research project and follow the literature research task that would be required by responsible engineers and scientists. Let's assume the project is to determine the vulnerability of typical aircraft electronics to lightning-induced voltages. The contract, in our imaginary portrayal, is with the Air Force and is of course DoD.

Your company library will register this contract with DDC in approved fields of interest. Request for bibliographic retrospective literature searches will be sent to DDC. After a few weeks, the investigating engineer will have abstracts of studies previously completed that are in DDC.

However, approximately 50% of the literature never gets to DDC because some of the SPO's and PCO's are not aware of DDC and never see to it that copies go to DDC. This results in the duplication of studies because the original work is lost to any retrieval system. The country and the taxpayer suffer.

The investigating engineers would probably want to make a search of the NASA Scientific and Technical Information Center because they probably have explored this area in the past. But--NO--you will be told that you do not have a NASA contract and therefore do not have a "need to know" and cannot have access to their collection. Again, the United States of America and the taxpayer loses. The same story would hold true at the AEC information facility.

The only report literature you can get is that deposited in DDC or National Technical Information Services. The NTIS report literature will consist of some NASA and industry studies that have been released to the general public.

Now, getting back to your DDC bibliographies. Many of the documents you identify as being pertinent will have an "L" beside the accession (order) number. This means you cannot acquire it unless the SPO approves your request, because he is controlling the release of the document. The office the SPO was in may be gone; he may be reassigned and no one is around that can approve your request for the document. Again, you are defeated in your efforts to review the literature. The procedures established by bureaucratic agencies have locked out the ultimate user of the information and as a result our country cannot develop important capabilities or even essential weapons systems in the most efficient manner.

Your librarian will be busy making all kinds of searches for you, and of course I have oversimplified the searching technique. My main point is the inadequacy of the information centers in the government. They lack active acquisition programs and proper exchange of information. The procedures are a practice in red tape tangles.

My final recommendation as I address you as a United States private citizen working on a voluntary basis with a congressional delegation in San Diego, with the National Contract Management Association and their relationship with the library technical information specialists, is to make a firm stand on problems and recommendations to improve the network of information technology systems.

Don't go to DoD. Don't go to Transportation. Don't go to Agriculture. Make a firm stand as a National Classification Management Association and go to Congress as a society, not as an individual or a corporation. They'll scuttle you if you come in the name of a company you work for, but they will listen to you if you come as a group.

PRESENTATION BY MAJOR HOCK: Air Force Potential Contractor Program

What is it?

The Air Force Potential Contractor Program (PCP), as its predecessor, the Air Force Technical Objective Document (TOD) Program; the Army's Qualitative Requirements Information Program (QR1); and the Navy/Industry Cooperative Research and Development Program (NICRAD) is an information exchange program under which the Air Force will sponsor qualified contractors for access to the Defense Documentation Center (DDC). The key word to be stressed is "Potential" as the program is primarily aimed at providing access to information on DoD research and development programs in specific technical areas to those contractors who do not have current contracts in these areas. The intent of this program is to supplement--not to replace or duplicate--the required procedures of registering with DDC all DoD contracts under which DDC services are desired.

One point needs clarification as it is frequently brought out in correspondence and conversations regarding the PCP. The transmittal letter and instructions on the PCP were interpreted to mean the TOD Program was totally defunct. The TOD Program was titled such because a contractor's original entry into the program was based on the approval to receive Technical Objective Documents

(planning documents) from the laboratories. Technical Objective Documents will indeed be prepared and placed in DDC or the National Technical Information Service (NTIS) for secondary distribution. Air Force sponsorship for DDC services under the TOD Program was terminated upon implementation of the PCP. In essence, the PCP replaces that aspect of the TOD Program and henceforth the Technical Objective Documents, when classified, may be obtained under the PCP.

The responsibility for administration of the PCP is vested in the Scientific and Technical Liaison Division, Director of Science and Technology, Air Force Systems Command.

Eligibility for Participation

Basically, the PCP is open to industrial, educational, and non-profit organizations who have a demonstrable capability to perform work under a contract, or grant, with the Air Force. Approval for participation is based on three considerations:

1. Capability
2. Need-to-Know
3. Security

Capability is ascertained by an evaluation of contractor-prepared information that is performed by scientific and technical personnel in the laboratories. Factors evaluated are experience in performing work for the Government, personnel, and facilities.

Need-to-Know is equated to the possession of capabilities, the expression of a desire for information in a given technical area (COSATI field and group), and the execution of a policy agreement.

Security aspects of the PCP are controlled in a manner similar to that of contractual transactions and thus will be handled by Defense Contract Administration Services Regions (DCASR). Those organizations which do not have or desire to obtain appropriate facility and personnel clearances may participate on an unclassified basis.

What are the Benefits

It is unrealistic to suggest that the PCP is ideal and meets the desires of contractors when, in fact, it is more restrictive than the TOD Program and also requires a greater amount of effort and cost on the part of the contractor to qualify. Overall, however, the benefits to be derived appear to warrant the investment.

Access to current planning information, technology needs and research objectives provides insight into DoD research and development which could place a contractor in a more favorable position for future contract negotiations. This information could also be a driving force for orienting the Independent Research and Development Program (IR&D). There is also that aspect of a company using a military technology for application to a civilian problem.

One benefit of specific interest to the National Classification Management Society is a retention period for classified documents that is equitable to the useful period of documents.

Application for Entry into PCP

During February 1974, packages containing instructions and application materials were forwarded to each participant in the TOD Program. They are now available from the Air Force Systems Command (AFSC) Contractor Relations and Small Business offices (CR&SB) - eleven are located throughout the command--or from Hq AFSC--either the R&D Base Procurement Office (PPPR) or the Scientific and Technical Liaison Division (DLXL). Each package consists of the letter of instructions with the following attachments.

1. Roster-AFSC Organizations Related to Technical Areas by COSATI Fields and Groups
2. Sample of Supporting Data
3. Policy Agreement
4. Roster-Air Force Contract Relations and Small Business Offices
5. Roster-PCP Administrative Local Points
6. Appropriate Forms
 - a. DD Form 1630 - Research and Development Capability Index. Scientific and Technological Fields of Interest
 - b. DD Forms 1540 - Registration for Scientific and Technical Information Services
 - c. DD Form 1541 - Facility Clearance Register

All forms or prior edition thereof being utilized for this program with the exception of the Policy Agreement have been in existence for quite some time and for the most part self-explanatory.

Thus, only salient points--those frequently misunderstood--on the submission of documents will be presented.

The Policy Agreement is submitted to the laboratory that a contractor selects as his principal Air Force Contract. This principal contract should in most cases be the laboratory that has cognizance over the major portions of the technical areas of interest to the contractor. The contractor should also advise all other laboratories to which he submits an application of the principal contract. Frequently, the term lead laboratory is used. The roster which delineates the AFSC Organizations Related to Technical Areas by COSATI Fields and Groups was devised to assist in making this selection. If the contractor has signed a Policy Agreement with the Army or Navy, he should send a copy of that agreement with each application to Air Force activities. By mutual agreement each service will honor agreements executed by the others.

The DD Form 1630 and supporting documentation actually serve a dual purpose in those cases where the contractor, in addition to participating in PCP, desires to be placed on the R&D Bidders' Mailing List. For application to the PCP, portions of the DD Form 1630 and the associated supporting data are submitted to the appropriate laboratories for evaluation. To be placed on the R&D Bidder's Mailing List, the complete DD Form 1630 and supporting data is submitted to each AFSC CR&SB office and to the R&D Base Contractor Division, Hq AFSC.

DD Forms 1540 are submitted to and approved by the laboratory identified by acronym on the roster relating organizations to COSATI Fields and Groups. The contractor completes only Part I - Requestor Application except for Block 8, the expiration date. The laboratory, after evaluation of documentation, completes Parts III and IV, The Approval and Subject Fields of Interest portions of the form, and inserts an expiration date which is dependent upon the effectiveness date of the Policy Agreement.

Status of Program

Thus far in the program, the DD Form 1630 and supporting documents have been the biggest problem area. Contractors frequently have not included sufficient information. It must be realized that the burden of justification is on the contractor; poorly or inadequately prepared documentation is returned with a letter of explanation. It should also be obvious that the personnel performing the evaluations for PCP also participate in the source selection procedures for contracts.

The response to the program did not immediately meet the expectations; however, it is growing at a good pace. There are currently over one-hundred participants and additions average 5-7 per week.

In summary, the PCP was designed to be mutually beneficial to both contractors and the Air Force. To a competent contractor--access to information which could place him in better position to receive government contracts and to conduct relevant IR&D. To the Air Force--identification of additional qualified sources. While it is not the ideal, it does appear to be worth the meager investments.

PRESENTATION BY MR. KAHN

I'm sort of surprised at being the No. 2 man here. I was once in a minstrel show. I was in the chorus and I always wanted to be the end man, but I don't think I made it today, either. I have no formal presentation to make. My remarks will be completely impromptu and extemporaneous.

I'm really substituting for the Administrator of the Defense Documentation Center who couldn't be here because of a prior commitment.

I'd like to make a comment about our organization, the NCMS. Since 1969, I've attended these seminars, except for last year when they wouldn't let me cross the Potomac to attend the sessions in Washington, D.C. Actually, I live in Chevy Chase and work in Alexandria, so I do cross the Potomac every day but last year DSA decided that someone else should attend and for a non-government sponsored symposium the rule is that only one person may do so.

These seminars have always been very helpful. I come away with a feeling that my professional batteries have been recharged and I hope that this occurs to all of you.

On the matter of document retention, I wonder what I can tell you about DDC, how we fit into the picture.

When DDC receives documents, those documents are microfiched. That is, we put them on film and forever after, they're available to qualified requesters.

We can then furnish microfiche or paper copies. If two copies are submitted to us and if you want one of those two originals, you may be lucky and receive it within the first year, provided yours is the first request. We no

longer keep paper copies after one year, so the chances of getting an original copy of a document are diminishing.

After the one copy is sent out and during the first year, if you want a paper copy, we use our microfiche and reproduce one for you. Now, there's something to consider, that if we get a good document to start with and we get a good microfiche and if our reproduction equipment is in real tip-top shape, you get a real good reproduction from that microfiche.

I think that in this retention question we in DDC are really in the middle. We can't tell you one way or another what should be done on that score. This would be up to, I feel, the DCAS people. It seems to me that DCAS and the contracting officers ought to get together and make decisions on retention.

I might also tell you one other thing about saying if we have a document. We find that a lot of documents do not get to DDC, so that we don't have a hundred percent of what you might want. To repeat then, if you get the documents to DDC, we will put them on microfiche for you as well as for us.

The reason we don't get a hundred percent of the documents is that in a Department of Defense Instruction, 5100.38 (soon to be revised), it more or less gives the charter, the guidelines for DDC, listing categories of documents precluded from DDC. One of those categories--we've been seeing lately because the Security Regulation 5200.1-R, has a paragraph mentioning "sensitive methods and intelligence sources." DDC is not allowed to accession documents that have intelligence material, but as I read that regulation, it is very loosely set forth in that paragraph and I suspect too rigidly applied.

In the event we get such a document, we usually give you a telephone call and ask, "Do you really want this document to be in DDC or do you feel in light of the security regulation that it should not?" If you feel it belongs in DDC we'd like you to confirm it in writing to us.

I expected that after I heard more of the speakers that I would be able to answer some questions about limited documents, but I see that the speaker preceding me has already mentioned them.

We annually receive approximately forty thousand different titles, I don't mean copies. There is a great disparity between titles and copies. If you send us a document that is supposed to be

released to the public, we need twelve copies. All other categories, and this includes unclassified documents that have to be limited, or classified documents, we only need two copies.

Of our forty thousand titles per year, and that's a round number--I don't think we quite met forty thousand this past year--about thirty-five percent carry the distribution statement that limit distribution.

That distribution statement is the "B" statement. There are only two statements, you know, the public release statement, which is the "A" statement which goes on the unclassified/unlimited, and the "B" statement, which has to be on a document if it's unclassified and you want it limited. A classified document can be sent to us without a statement and in that case only security and need-to-know will control its distribution.

The 35% figure of document titles mentioned previously as being limited in distribution by the B Statement refers to 35% of the 40,000 total received. I don't have the exact figures. I calculated it yesterday, but I just can't recall it exactly at the moment.

I think that at this point I will let someone else get up and raise some questions, and, in the meantime, when we get a question period I'll be here. Thank you.

QUESTIONS AND ANSWERS

MRS. CLIFTON: Unfortunately, one of our panel members, Bill Jones, had to leave to be back in Los Angeles, so he sends his regrets. Now we'll have the question and answer period.

MR. JERNIGAN: I'd like to make a statement instead of a question, Joe Ann. My name is John Jernigan. I'm with the General Electric Company in Philadelphia.

As everyone in this room knows, classification retention, or classification material retention has been cussed and discussed for many years, and for as many years as notice has been brought to the attention of DoD, nothing new has come out of this.

You submit a request for retention and in ninety-seven or ninety-eight percent of the cases you automatically get retention for three years.

No one questions to any degree why you need the materials, so all you're doing is going through

a paper work mill, and even on the second request, if you show any degree of trying to reduce the number of documents, all material in your possession, you usually end up getting retention authorization for a second retention period.

I'm sure that Bill Jones has expressed the concern and feeling of everyone here today about retention, but if they let the security managers handle the retention, we will do so in a professional manner.

We sure don't want the material around any longer than what is absolutely necessary to do the job. However, if we continue to destroy the technology that we have attained over the years, we are going to destroy everything that we've ever worked for, and we're going to end up spending more money either going back to DDC if they happen to have a copy of the material, and having it reproduced.

Now, Bob Green has stated that new--or something is being done about this and a significant change can be expected in the very near future.

I know I for one sure hope so, because in our business in the past we have destroyed material one month and found out that an agency wants access to it the following month.

MR. CHELIUS: For Major Hock. The technical objectives program has a number of line items in the classified section. In other words, you have a number of separate classified problems that you want industry or organizations to begin to consider in solving those problems.

What have you considered as putting out; what have you considered with respect to also putting in with these TOD documents a security guide so that when companies generate information or submit an unsolicited proposal pursuant to these requirements that they will have adequate guidance in order to classify the information?

MAJOR HOCK: Well, we anticipate quite a few unsolicited proposals under this program. Really one of the aims of unsolicited proposals is to look for solutions to the different problems that are identified in the TODs.

Now, on the whole, most of the TODs are under-classified. We're talking down in the basic research, exploratory development and some in the advance development. When you're getting down to that stage, most of it is unclassified as you're talking about technology.

When you relate it to a system, you're getting up into the engineering development and usually at

that time you don't receive too many unsolicited proposals. Those you write out in a complete statement of work.

Now, if you do get a classified TPO and you reply to a certain TPO with a number, I would use the same classification as was on the TPO.

MR. CHELIUS: Maybe I should restate my question then.

How does your program relate to the overhead cost under, I think, ASPR Section 15 with respect to independent research and development?

MAJOR HOCK: This is separate from IR&D. This may be the driving force of the IR&D where we outline what we're looking for.

I would suggest that if you look at these TOD's and you find an item of interest, they will also give you a point of contact for that item. You get a contact down in the laboratory. If you do call that guy, indicate that you would like to put in a proposal. You might discuss it with him for a few minutes, or maybe make a trip down to see him and state "You're looking at it from this way. What do you suggest? Do we have grounds for an unsolicited proposal? Are we proposing anything new?"

MR. CHELIUS: What about a classification basis?

MAJOR HOCK: A what, sir?

MR. CHELIUS: Classification basis?

MAJOR HOCK: To that I can say only if the TPO within the document is classified, I would use the same classification. We hope one of these days--I think Mr. VanCook talked about it--that DDC would have the classified guide for all these weapons systems. If it is related to a weapons system, you would have a security guidance.

MR. BAGLEY: Jim Bagley, Naval Research Center. I would like to point out, however, that you're entering into a very interesting little legal problem in the sense that the Government cannot classify any information until it takes title to that information, and taking title means then that some sort of a contracting process has begun, so please, I would rather you not mislead the people. A true unsolicited proposal cannot properly be classified unless the Government has had title to that information.

MAJOR HOCK: Once you sign a contract, right.

MR. BAGLEY: I didn't say that. I said starting the procedure process.

MAJOR HOCK: The gentleman is right. Most unsolicited proposals we receive at the laboratory come in under company confidential, company proprietary, or something like that.

MR. BORMANIS: Joe Bormanis. I think I'd better start my question with a statement first. I think in most companies we have large libraries and computer tapes of various kinds. Also, computer print-outs. Normally, they are kept differently from the standard libraries we have. Has a library council ever looked at consolidating all information in one given technical information center of the committee with the data processing people from their own libraries, because, in most cases, if we need information, their indexing is so poor that you wind up running tapes for hours, maybe even days, till you find what you need.

MRS. CLIFTON: This is something we haven't addressed ourselves to, but it sounds like a very interesting future problem, very interesting, indeed. In essence, you're saying that you have information that your data processing section has put together and really supported an index, but you can't really find anything; is that correct?

MR. BORMANIS: Correct.

MRS. CLIFTON: We don't have anything as such like that in our company, but I can see the problem springing up. We haven't really addressed ourselves to that problem, but one of the problems we have had, we mentioned, is about how difficult it is to put classified information on the tapes, because it's impossible, so I understand, to erase the classified information.

At least my data processing people have relayed this to me, but then they told me a few other things that they couldn't do and then I went out and found out that they could, so I don't take anything that they say literally, particularly about the tapes. Is that true or not true? Does anybody in the audience know?

UNIDENTIFIED SPEAKER: Well, our tape system has classified material on it, but it just comes out, you know, that the title is then classified.

MRS. CLIFTON: You only put the unclassified portions of your cataloging information on there?

UNIDENTIFIED SPEAKER: Right

MR. CAMPBELL: I think you can remove any information in that tape that you put in it, but you'd have to be able to find it and address it and bring it out again, same as changing any cataloging of information, but all systems I know of do avoid putting any classified information in that tape. You have to go through too much trouble to handle it.

MRS. CLIFTON: I understand that you can't change the imprints on the drum. Myer, you should have some information on this. I'm sure you must be doing this at DDC.

MR. KAHN: No. I do know that when we have to change our records, you do it by specific fields, and if we have a set of descriptors, there may be eighteen or twenty or something like that we have to wipe out the field completely and write the whole thing all over again, leaving out what we want left out.

MRS. CLIFTON: But you have no problem with erasing classified information?

MR. KAHN: No, we just pick the computer field that it's in and we have thirty-six fields for each document.

MRS. CLIFTON: Okay, fine, Myer.

I have a question I'd like to address to anybody in the audience, because it's a question that comes up all the time and maybe somebody here could give me an answer.

We constantly run across retention problems. They tell us that after five years that much material is no longer valid and no longer of any value at all, and on retention of some of our reports this time around they gave us an additional three years on some material that is currently five years old, and they said at the end of the three years that we had to destroy it, because it would no longer be of value. It would be obsolete--so to speak--and yet my question is--because we found that the men in our organization would like to retain this because they claim quite the contrary, it is still quite valuable information, so my question is why, if the information is no longer that hot--is it still going to be classified three years from now?

Does anybody have an answer to that? We run up against this all the time, particularly in relation to classified journals.

I'd like to have some ammunition to use when the subject arises. I don't understand why they shouldn't declassify it.

LT. COL. GRIMES: I'd go in and ask them under the Freedom of Information Act to review it. If the document is confidential and it is five years old and they're going to give you three more years, then they've got to go back to a top secret authority and get permission to exempt it, or they have to give it to you. One of the two.

MRS. CLIFTON: Thank you very much.

UNIDENTIFIED SPEAKER: They could be exempt by statute. It might be restricted data.

UNIDENTIFIED SPEAKER: Can't hear the lady.

UNIDENTIFIED SPEAKER: The material could be restricted data and, therefore, exempt by statute from the classification or downgrading.

MRS. CLIFTON: My point is why would it be restricted data?

UNIDENTIFIED SPEAKER: By statute.

UNIDENTIFIED SPEAKER: As a librarian, I also have a question.

MRS. CLIFTON: Please state your name.

MS. ALEXANDER: Colleen Alexander, Convair. In declassification of microfiche, which is getting to be sort of a new thing because we haven't had fiche that long, but, again, when you go to declassify a piece of microfiche, no one seems to be able to tell me how to do it, and I don't want to destroy it and then buy it back declassified for a dollar and a half.

MRS. CLIFTON: We're also having this problem.

UNIDENTIFIED SPEAKER: I'm going to ask a DCASR to back me up to make sure that I don't say the wrong thing, but I think if I had a sheet of microfiche and it was due for declassification I would put it in an envelope or a container and put all the downgrading instructions on it. Then, whenever that was removed from files for a hard copy to be made, the hard copy would then have to be declassified in accordance with the instructions on the envelope.

If the inspector comes in and pulls it out of the files and says, "Why don't you declassify it," literally, you would have--because in the manual it provides for marking on the container, the envelope, the box, or whatever the thing is in, and I think this would probably be the simplest solution.

If you have a long reel of film and perhaps only certain things within that were declassified or downgraded, again, you'd have to put the instructions and what you were doing on the container and then transfer that to the hard copies as you used it.

MR. CAMPBELL: There is, I think, precedence for doing something like you say. The microfiche is one piece and you declassify that piece with the statement that if it is distributed to somebody, it must bear the proper markings. There is a statement that one can use, I believe, on the micro piece envelopes to the effect, that is, if the document is blown up into hard copy, each piece must be properly marked before you give it to the recipient, and in our company we also mark the piece itself with a confidential or unclassified, whatever the marking is, so that if the fiche comes out of the envelope, we do know what it is.

MRS. CLIFTON: Myer, would you respond to that, also? What do you do at DDC? I could have gone all right without asking that question, I'm sure.

MR. KAHN: Once again, I'm not in that division. I have seen our people take the microfiche, and where it says confidential, they mark it through. I don't know exactly what they mark it with. I have also seen them take the microfiche and strip over, you know, like a correction tape--you make corrections on it when you type, and put an unclassified on that, and then we also mark our cards in our shelf list.

Now, we don't change the AD number if it is declassified. It retains its original AD number. We do change the code in the computer whenever this is run out in a bibliography.

MRS. CLIFTON: Excellent. I think we had a question back there.

MR. GREEN: No, as a matter of fact, I don't have a question. Bob Green, DCAS. I'd like to just address a couple of things here.

I said from the podium that I wasn't going to get involved in the details of things which we have cooking in the industrial security program.

However, I am, since you've shown so much interest in this question of retention, and I'll trust your good judgments and faith not to make me come back and eat my words later on.

First of all, in the ISR, there's a very clear statement of DoD policy with respect to retention

of classified material in the hands of industry. It says that USER Agencies should take a liberal approach, are encouraged to take a liberal approach.

Will you quote the rest of it, Jim?

MR. BAGLEY: Not quite, but I have a recommended change.

MR. GREEN: The philosophy--I won't go by the words, because I'll be corrected on the words--the philosophy is you take a liberal approach because it's considered by the DoD. The retention of this technical material by industry contributes to the long-range requirements of the DoD.

It keeps current and it adds to the technical expertise and knowledge that's held in industry that we depend on so much.

Now, we have an ISB, an Industrial Security Bulletin, coming up very shortly, I believe, to the USER Agency which reemphasizes that DoD policy retention is a problem to us as it was to you.

In that article, we are stressing the role of the UCASR in assisting industries in obtaining retention authority from the USER Agency.

Now, we can't determine in all cases the need for industry to retain. That is a USER Agency decision, but where the reluctance to allow you to retain is based on a lack of confidence in your ability to protect, a lack of confidence in your disposition systems, a lack of confidence in your ability to downgrade and declassify property, we can support industry in virtually all cases.

We can support industry by certifying to the USER Agency that this facility, this company, has demonstrated to us through the industrial security program that they can protect a due downgrade, they do destroy properly and there is no risk to security to allow this company to continue to retain. That's one point.

A couple of the things that we have under consideration, and, again, please don't say, "Bob Green says this is the way it's going to be," because before you see it, it may take a hundred-and-eighty-degree turn. That's why I'm very cautious on making any comments on the details of proposed changes.

We have under consideration a change that will require or at least afford an opportunity for the USER Agencies to authorize retention in the DD Form 254. If it's known that the material will be made available to a contractor or obtained by him, only if the performance of a contract has continuing research value to him and furthers his position of being able to deliver to the Government, the retention can be authorized in the 254's. That's under consideration.

Another feature of retention that we have under consideration is allowing a contractor to retain classified material that is developed for bid purposes, whether or not he is the successful bidder. That material has value to the company. It is valuable to the Government. It puts him in a better position to bid on future procurements.

One other thing that I'll have to confess is that my memory is very short. I know that NCMS has made one or more proposals to Mr. Liebling's office on the overall question of retention. That was going to be my question. I have lost track of those.

MR. BAGLEY: The proposals have been made. Both have been denied, and I learned just this morning that the retention position papers that we had put in were virtually the same as that recommended by the Library Council.

MR. GREEN: So what we are faced with in the industrial security program is, based on our experience with the industry and with USER Agency, is trying to relax to the maximum extent those requirements for continued authority to retain from the USER Agency by either making it automatic in some of the ways I've suggested or for at least extending the periods if we still have to go through the mechanics of getting authority periodically to extend those periods of time.

Thank you very much.

MR. SUTO: One of the items that Bob mentioned here, authorizing retention in the DD 254, is the one area that contractors can really contribute towards writing or revising the DD 254, and if they're asked, for example, to provide some input into the DD 254, this is what they should do.

They should ask for the retention of the material for a certain period upon the close of the contract. You can probably do this ahead of time and save yourself a lot of extra paper work.

We have done it on occasion. It has been approved.

MR. BAGLEY: Jim Bagley, NRL. You were talking earlier this morning about reference material and the inconsistency, shall we say, of definition of what reference material is, and you brought up one particular point which I have been very concerned about for a number of years.

Now, somebody mentioned Shock and Vibration Bulletin which NRL distributes, but NRL does not have title to all of the information in that. So when people ask us for a retention authority and we do not have current contracts, the action that my office has taken to start with is to write a letter to the DCASR, the appropriate DCASR, with a copy to the requester and say, "We know that this company is still in business. We know it is doing work in the area. We also know that the information in these bulletins are probably the only reference source, or at least one of the most authoritative reference sources that exists in the area. Therefore, we recommend that they be given indefinite retention authority as long as they still have a clearance and storage capability."

Now, this is done. It's the kind of thing that you do to get around the specific situation.

There is another point, I believe, that should be addressed, and if you pardon me, Bob, I was looking at the words specifically yesterday. That's why I was able to quote them. The USER says, "Shall be encouraged to take a liberal attitude." I think it's the set of words, "Shall be encouraged," which may become a hang-up, so I think that some considerations should be given to a recommendation which says, "USER Agencies shall take a liberal attitude," rather than putting the qualifiers in there of, be encouraged to." It's a play on words, if you will, a matter of semantics, but I think the fact remains--and you people in industry are better judges of this--that procurement agencies, once they get a contract over and done with, care less about it. It's over, and the residual things like audit, what may be retained and so forth, gets thrown into the past, or else new people take over, so, therefore, there is a tendency, in spite of DoD's words, to hold back, to wonder, to why, and all of the other things.

I believe that if the words were put in a more positive sense without the qualifiers, then you might tend to see a change of attitude, but that's only one other suggestion.

MR. JERNIGAN: John Jernigan, G.E., again, just to expand upon what Jim has said here, that when the contract has been completed, the first thing they tell us is that they want to close out their records.

MR. BAGLEY: Right.

MR. JERNIGAN: Now--so you go back and you explain to them--you can talk to them, or verbally, or through written correspondence, and you explain that you still need access to this and they say, "All right, if you still need access to it, you transfer it to a related program. We will authorize the transfer if you get another contracting officer to accept it."

You can run into hang-ups. By this I mean you could be working on many programs, but none of which are related to the specific subject of the previous contract, so you're in a bind.

So they say, "If you can't transfer it to the related contract, destroy it."

Now, we're talking to contracting people that really have no concept of--or I don't feel they have any concept after talking to them--of the technical knowledge that exists in these documents.

Who--and I repeat, who--is in a better position to determine the technical value of a document than those people who work with it on a continuing basis?

So there has to be some other way, because if they want to close out their contracts, you've got a problem. You also have a problem if you want to keep documents on an Air Force contract and it happens to be a Navy document or vice versa.

MRS. CLIFTON: That's for sure.

MR. JERNIGAN: So you've got to go across lines, and sometimes this is pretty hard because the Navy says they don't want the Air Force to know what they're doing, so never the twain shall meet.

MRS. CLIFTON: That's right. I believe Mr. Berry has a statement he'd like to make.

MR. BERRY: In the area of reproducing microfiche, DDC does not make new microfiche or upcheck their records except what they have--what we'll call a tickler file. When a request comes in for a specific document that's either a downgrade where the distribution statement says change, they will then change their microfiche and give you a new one, but they do not go back and upcheck all their records automatically.

So this is very important to you if you're an industrial security man and your company tells you you have to go down and work on all these documents. They'll think somebody is crazy, because what happens when you go from microfiche to hard copy in DDC, they only change their front and back cover. They do not change all of the individual pages.

That's another thing you ought to take into consideration, and as far as the retention is concerned right now, if you do not have a contract that you can specifically tie the documents back to, the industrial security manual says that you will have to get rid of those documents.

That's the instructions that the inspectors have, so let's not kid ourselves and make words up of wisdom that's not going to work.

You must tie the document back to a specific contract or you must get rid of the document, and that's the way it reads now.

If you want to challenge me, fine. I'll pull out the ISM and we'll look it up ourself.

MRS. CLIFTON: This gentlemen here.

MR. HERRINGTON: Warren Herrington, Stanford Research Institute.

I've been there eleven years and we have obtained retention authority for every document we ever needed to retain, and there are methods of keeping them without tying them to contracts.

Now, it is true that we may have to go over and above the immediate ACO. We do not panic. When the DCASR people come in and say, "Why do you have all of this," they're asking a question. They cannot tell us to destroy it. All they're saying to us is questioning the number of copies.

We do get retention authority when we really need it. What we found we have to do is get the scientist, the engineer, the whatever you want to call him, to give us some of the words that will explain the need therefor, rather than going out with some stereotype request.

We find when dealing with Government people that eventually we will come across someone who has a reasoning ability. Now, you may have to go through several channels to reach that point--I will concede that--but you can. It takes a little perseverance. If you need it, you can end up doing it.

UNIDENTIFIED SPEAKER: Amen.

MRS. CLIFTON: This other gentleman back here. You had your hand up.

MR. FLORENCE: Here, may I go to the platform?

MRS. CLIFTON: Surely.

MR. FLORENCE: We've got a problem here that I think has been referred to as one of the long continuing problems of industry on retaining material in past classification markets. With all due respect, the problems are short.

I do want to come up and make a comment that I believe will give some guidance to this society, reorienting itself as an organization and approaching the resolution of this problem, and I think I would like the record to show at least a few of the individuals are gone now but the record should show a little matter of history that I think would help resolve this problem, and I have in mind going back a few years in my experience when the question of disclosing classified information to people outside the Executive Branch or outside of the Government, in industry, or whatever you want to call them, with the question to be resolved on the basis of what all of you like to call, "Need to know now."

Contracting was absolutely no consideration. The basis and the policy on which we in the Government disclosed classified information to people outside of the Government was who were helping us in a particular project. Contracting was only a representation of a defined procurement. We disclosed information to serve the Government's purpose and we were not encumbered with all of these procedures--God wish they were contracts.

Through my experience, I began to see again a few years ago that there had to be a simplification of the industrial security organizations, and this being industrial firms had had material that had been disclosed to them or at least for them to use that were marked for classifications.

Those who were visiting industry in the guise of industrial security specialists were the ones who created more than anyone else the idea that an industrial security manual, a contractual document, that those procedures had to apply to all classified information held in, say, an industrial firm.

The contract manual itself for many years referred only to contract orders. I, myself, was one who I think generated more than one individual the need to make this manual apply to things other than contract information.

It was changed a little bit, but this is to mention only to show that there is so much discussion about the use of Government classified information in terms of contract requirements.

John Berry just mentioned that if there's any question about your holding classified information now, the concept is all imbedded in these contract procedures, and a little old Industrial Security Manual says if you don't need that information, you have to get rid of it.

This actually is a contradiction of the Government's interest in the industrial support being able to provide for the defense of this nation. The Government is full of people who would love to see to it--and they do, as Warren indicated for Stanford Research--the Government is full of people who would like to see that the potential for the logistics support of our national defense means is kept as strong as possible, and where there is any necessity whatsoever or any desirability that you in industry retain the material necessary to provide you with the basis for supporting the nation, you will get the information.

Now, my message to NCMS is to reorient itself and make representations in the name not of contractors, not of industrial security, not in terms of these procedural matters that John Berry so aptly referred to a moment ago, but raise your sights to providing for the defense of the United States, and if there's necessity, the Department of Defense agency can provide a different kind of a vehicle for the use of material bearing the classification mark, and I won't give it the term classified material, because a lot of it really isn't, just has classification markings, but if there's necessity for a Department of Defense collection for the use of material for defense purposes, fine. You're always going to have trouble to try to cram that into a contractual document.

I suggest that NCMS look at that.

MRS. CLIFTON: I didn't get your name.

MR. FLORENCE: Bill Florence, self-employed, free-wheeling.

MRS. CLIFTON: Thank you. We have a lot of free-wheelers here today.

Are there any other questions?

In closing I'd like to say that it's really been great to see you people here and to know that you are concerned with our problems, because sometimes we've felt we're all alone in this

battle. With that, I'd like to say it's been a real pleasure to come to your meeting and share our problems with you and our thoughts on how to solve them. The interaction between our groups will, I hope, be very productive.

PANEL: INTERNATIONAL SECURITY

MR. A. A. CORREIA, Moderator
Rockwell International Corporation

MR. E. M. SILVER, Panelist
Manager, International Governmental Liaison,
Hughes Aircraft Company

MR. E. T. BROWN, Panelist
Manager, Licensing, Rockwell International

MR. RAE NEHLS, Panelist
Field Management Division
Office of Industrial Security
Defense Supply Agency

PRESENTATION BY MR. SILVER

Yesterday morning, as I was motoring down to San Diego, I heard a very interesting news item on the radio.

It seems that in San Francisco, the City Councilman in reviewing the City Code, found that it is against the law for ugly people to appear on the streets of San Francisco, and therefore, are repealing that City Ordinance.

I would like to suggest that there are other governmental organizations with laws, regulations, et cetera, that perhaps should be reviewed in this same light.

You know that the kids are all out doing ecology. The boys are gathering newspapers for recycling and the girls, aluminum cans, and now we are told to recycle everything in the interest of saving our national energy. The idea of recycling is not really new.

The Federal Government invented it a long time ago. From an international aspect, they have been recycling requests for foreign disclosure of information for years.

The logic of this seems to be that the more times you can review or recycle a disclosure request, the better the decision is going to be. The fact that identical information was reviewed last year by an equally competent, if not the same, group of people, and the year before that, and the year before that is of no significance.

About five or six years ago, the Office of Munitions Control (OMC) decided that even though everyone had been operating apparently very well, using the non-renewable disclosure Authorization Letters for the export of classified data, that this should be changed and that we should use a license renewable once a year. In order to renew this license, one would have to go through the same basic processing procedure that was followed on the initial application.

What has happened as a result, is that each time you go back for a review, you must first approach the Contracting Officer for permission to republish and redistribute the classified document. This provides an additional opportunity for Contracting Officers to determine what the national policy is going to be for the foreign disclosure of classified information. Without the Contracting Officer's approval, you cannot go to OMC to get your license in the first place.

Let me make it clear that I'm not discussing the disclosure of unclassified technical data which OMC also controls.

This discussion is directed principally to the disclosure of U.S. classified information to foreign governments.

We enter into a recycling through Contracting Officers with the Contracting Officer on a fairly low level of determining what the policy of the U.S. Government is going to be in the disclosure of a specific classified document.

Because of this constant annual recycling, we find ourselves strapped with a time problem in addition to the requirement of going through so many reviews in getting an approval to begin with.

Even after a classified system or a piece of classified equipment has been sold and delivered, we still find a processing difficulty in obtaining permission for representatives of the same foreign government to come to the United States and carry on classified discussions with us as well as for supplying them with classified brochures regarding their newly acquired equipment.

The regulations for the retention of classified material for which foreign disclosure has been authorized are identical as an across-the-board application of the rules for governing U.S. classified material, which is held tightly under the cognizance of the Contracting Officer.

Once the material has been sold abroad or classified documents have been exported by the U.S. Government, it is strange that the retention and reproduction abroad is of no concern, but in the U.S., all the rules for the handling of classified documents still apply.

The other night, I was commenting to an individual that we could be faced with a situation where the Contracting Officer would not permit us to retain classified material in our company files, but if the same U.S. classified material had already been exported to a foreign government, it might be necessary for us to go abroad, visit the foreign government to have access to the U.S. classified material we developed, but for which the Contracting Officer could not foresee any future.

I think that there should be some consideration given to all material which has been approved for release to foreign nationals. Maybe the same rules should not apply.

Perhaps your marketing organizations are very meticulous in preparing their marketing brochures, but where I work, occasionally we will prepare a marketing brochure, we will go through all the procedures and obtain a license to export the document, we will have the document placed in the hands of the foreign government, only to find out that there was something objectionable in the presentation. It is to our advantage to completely revise the format, particularly some of the unclassified information in the brochure. The level of classified technical data in the revised brochure is to be identical. The problem is, we have created a new brochure, a new classified marketing device, and we must go back to the very beginning. We must go all the way back, starting all over again with our processing, as if we had never been through the circuitous route.

Two arenas where the disclosure of classified material is performed under the direction of the U.S. Government are the following: One is the release of documents abroad, the export of documents via Government-to-Government channels based on an export license. The other is visits by foreign nationals to our U.S. plants. There has been no correlation between these two activities. The Air Force recognized the redundant staffing for identical information and have stated in their visit approval letters that if the Contractor already holds a munitions license for the disclosure of the specific U.S. classified information involved in the visit, that their approval is granted for the discussion of that same material during the visit. The interesting thing

is that even though this letter is an enlightened approach to the handling, the procedure that's being followed is not in accordance with the regulations the contractors are required to follow in the Industrial Security Manual. The Industrial Security Manual provides for certain routes that these letters of approval must be sent through, and that they are to specifically state the level and scope of the classified information to be released.

Based on Paragraph 5h of the ISM, one must obtain approval to incorporate U.S. classified features in a foreign proposal. Additionally, in Paragraph 5p of the ISM, publication and distribution of classified sales literature (this is interpreted to mean all U.S. classified documents for which the Contractor requests release) is controlled by the Contracting Officer.

Between these two acts, you can see that a Contracting Officer has the opportunity to administer decisions affecting U.S. foreign disclosure policy on specific U.S. classified information.

I don't know that there is any appeal route, but unless your brochures have satisfied steps 1 and 2, the State Department will not accept your request for an export license.

If you have been successful in going through steps 1 and 2, then you go to the Office of Munitions Control. Within the Office of Munitions Control, a very detailed staffing and review of the candidate classified document takes place. The Office of Munitions Control makes no unilateral decision, but bases its decision on the positions of the various military services, including DDR&E and other governmental organizations.

The User Agencies of the same Contracting Officers, which have just finished reviewing the same document under steps 1 and 2, again review the identical material.

So far, the same document has been cycled through at least three reviews by the same User Agency.

During this time period, if the same foreign nationals that we have processed a document export approval for were to request a visit to our facility, they would have to submit a visit request to the three military services. The three military services would have to go through an independent staffing to determine the releasability of the identical information for classifications at our facility.

These two steps are apparently independent and there is no cross-over or coordination. Each request for classified discussions at a U.S. facility is determined on a case-by-case review, independent of any existing Munitions Control case or prior visits for the same access.

Let's now move into the phase of marketing where a whole year has gone by and we haven't obtained a contract. The license that we hold for the release of classified material has expired.

We want to pursue our marketing efforts by sending some more of the same documents to the same foreign country. We must start all over again as if the first year had never existed.

Basically, the Contracting Officer only approved the publication and distribution of this classified document for your initial stated distribution.

We go back to the same Contracting Officer to get permission to publish the document to send it to the State Department again, since our license was only issued for one year. You are also in trouble because Paragraph 51 requires disposition for classified documents generated in connection with unsuccessful marketing attempts.

Let's presume that sometime in the second year we become successful and obtain a contract. Not only did we obtain a contract, but let's further presume that it is for software and the delivery of hardware. We need a different license now, a license that describes the specific piece of hardware or pieces of hardware that are to be delivered to a foreign government.

Again, you must go back to the State Department. In order to explain to the State Department what this hardware is, it is generally to your advantage to include some brochures that describe it.

Where are you going to get the brochures that describe it? Go to the Contracting Officer and ask him for permission to republish the same document again. Also ask him for permission to distribute it to the State Department again, and once more you're off and running.

You've got your hardware export license. The hardware export license again is only valid for one year. The hardware that you're going to build is not to be finished for, say, a year and a half. You have your choice of either waiting about seven months and then going in for an export license, or you can immediately go in for an export license.

At Hughes Aircraft Company, we don't like to go out and spend a lot of money building hardware if we're not pretty certain that we are going to be able to export that hardware when it's finished. Our approach has always been, even if the hardware won't be shipped for two or three years, that we want a security blanket, so to speak, of an export license. All during the process of building the hardware, subcontracting for the special parts, spending the overhead dollars, etc., we must know our chances of being able to deliver the hardware.

Continuing this development to the next logical step, we get into a licensing agreement where we're going to allow the manufacture abroad that involves U.S. classified information. Again, you go to OMC, but this time with a proposed license agreement which specifies which sales territories are to be included, what the product is, where it came from, which military organization has cognizance. Preferably, OMC would like us to again include some description of the classified information that's involved, so once more, we go back to the Contracting Officer to get permission to republish the very same document.

Now, a very interesting thing happens. When we reach this point, we almost receive a carte blanche export authority. Once we obtain an approved License and Technical Assistance Agreement that involves the disclosure of U.S. classified information, no longer do we need to go back to the State Department with the DSP-85 request for the release of technical data as long as it was described within the scope of the approved manufacturing agreement. Not only is this good news, but our approval probably extends over the next several years.

But wait, there is still a requirement that you notify the Contracting Officer whenever classified material is sent to a foreign government according to the Industrial Security Manual, Paragraph 17e. Even though we now have this approved License and Technical Assistance Agreement, or have a broad blanket approval for the release of technical data abroad, what happens when our foreign licensee visits our facilities? He still has to write a visit request. He still has to identify the information he wants to discuss. The visit request still has to be processed individually by each of the military services.

Now comes the time for closing the contract. Here's where we get into an interesting discussion. If we are working on a License and

Technical Assistance Agreement and the licensee issues contracts for us to provide certain assistance when these individual contracts close, must we obtain retention approval for our classified material?

If by this time the U.S. Government has declassified the material, the only classification the material carries would be a foreign classification. Even though it's a foreign classification, the rule is that you protect their classified material in the same manner as U.S. classified material and so the same rules apply. We can be faced with the situation of going to our foreign customer, who holds the information, based on our license agreement, and asking him if we can retain our information that we generated, but which he classified. Not a very realistic approach.

Basically, the foreign governments are not so concerned with retention of classified material as the U.S. Government is. Their attitude is, they want their programs to be supported. They want to be able to call on a contractor not only to support equipment they are actively acquiring, but they want after-sales support and proposals on how to improve the equipment. Their concern is rather will we have adequate information to support them, not that we're going to have too much. Their attitude is that the cost of storing material will be sufficient to motivate contractors to get rid of all the unnecessary information.

We always want to be able to take information, in which we hold a proprietary interest, to the Office of Munitions Control for an export determination. Because of the hopeful time-phased declassification of most U.S. information, we must be permitted retention for information necessary to support possible foreign sales and necessary release requests.

The recommendations. Now that I've torn the program apart, let's rebuild it. The recommendations: Get the Contracting Officers out of the loop of being notified each time classified material is being sent abroad. Out of the loop of reviewing classified material for publication and distribution. Get them out of the loop completely on international operations.

In place of the Contracting Officer, still maintain the Office of Munitions Control which, as I explained earlier, coordinates all of their actions through the military services, which represent these Contracting Officers.

Once classified material has been approved for export, stop the requirement for the annual Office of Munitions Control renewal and go immediately to

the situation that I described for the license and Technical Assistance Agreements. Once the material has been exported or once we have an approved level for disclosure of technology, let's stop recycling the approvals over and over again.

Permit classified visits in the United States, based on an export license or Technical Assistance Agreement. Under this, the foreign national visitor would go to his government. His government would certify that the foreign national is indeed cleared. The foreign government would notify the contractor via the U.S. Government, but the staffing of determining what has been approved for release or what hasn't (the requirement to have--as one of the military services does--a military representative present during the visit), would all vanish. To show you the fallacy of this requirement to have a military representative present during a classified visit, let me explain that under the terms of the Industrial Security Manual, we can send our marketeers to a foreign country and we can disclose and discuss U.S. classified information contained on that export license without any U.S. military representative present and without any other approval. In effect, we have greater latitude and freedom in carrying on U.S. classified discussions in foreign countries than we do here in the United States.

Abolish the U.S. Contracting Officer retention requirement for all U.S. classified information for which an export license has been issued. We have permission to export classified documents or they have been exported; let's stop the requirements of retention and transmission notification.

Let's avoid having to ever send our personnel to a holder of one of our documents in a foreign government because we could not get permission to retain the classified document from the Contracting Officer.

PRESENTATION BY MR. BROWN

There's an old saying that goes something like, "It's easy to dislike someone you don't know." Now I'll be the first to admit that I didn't like classification managers as a group--nothing personal mind you--it was because they represented a stumbling block on the road to progress in the conduct of business--at least that's the way I used to think.

When Tony Correia approached me to be a panelist at this seminar I thought, "Oh boy, here's an opportunity to really tee off on these guys who

keep telling me what I can't do!" It's a good thing I used the expression "tee-off" because it reminded me of what happens when I use that mental approach to playing golf--I either wind up dribbling the ball just past the ladies tee or I go screaming out-of-bounds.

So, like golf, I decided I had better find out a little more about the game before getting on the course with the club pro. It's obvious that I'll never play the game as well as the pro, but I will at least understand what he's talking about when he tells me how to improve my game.

I started by reading the Proceedings of last year's National Seminar and was very impressed to note that the major portion of the discussions related to ways of combating over-classification, resistance to declassification and cumbersome administrative procedures. It takes a highly motivated classification manager to challenge the need for classifying information when it is so much easier--and safer--to classify it "just in case." Besides the cost associated with his decision doesn't come out of his pocket or his operating budget. When you balance that against the classification manager's basic responsibility of protecting the nation's security and of interpreting the myriad of policies and procedures on the subject, you can begin to understand his reasons for caution and conservatism. Again, I liken it to the game of golf--each shot is different and the opportunities to screw up are unlimited.

When you look at international security, all of the problems are "doubled in spades." While the guidelines are well established for determining just who are our friends, our enemies or neither, we will all probably agree that while we may have common goals with them, none of our foreign associates have the same motives and objectives as the United States. Perhaps this is the reason there is leaning toward ultra-conservatism in the release of data--even unclassified/unlimited data--to foreign associates.

The result is a dichotomy. We have a national policy aimed at increasing foreign trade to improve our balance of payments position. Our experience indicates that this can best be accomplished through the medium of high technology products, a large percentage of which (especially in the electronics industry) had their origin in military developments or in company financed independent research and development projects which requires that any product or data that could be used for military purposes--generally those things listed in the International Traffic in Arms Regulations or ITAR--requires export license

approval. Additionally, anything developed in a defense industry that is not obviously in the public domain is considered military information defined as unclassified/controlled by the cognizant military organization for that plant.

My panel colleagues who preceded me have indicated some of the problems of double and even triple jeopardy in getting export approval on the sale or licensing of military products to friendly foreign military customers. I think there is an equally serious problem in trying to promote foreign trade in high technology products; it becomes monumental when you try to promote trade with the USSR and other Socialist countries in support of the current environment of detente which is aimed at relieving the tensions and hazards of the cold war.

What are the Soviets interested in? High technology! You guessed it--military/aerospace oriented industries where the government and industry invest heavily in technology development. One factor that I believe a lot of people do not appreciate is the fact that Russian scientists are on a par with the best in the world and they are fully aware of world-wide developments in scientific discovery--they have done their homework well. The area in which the Soviets seem to have difficulty is in applying scientific knowledge to the solution of a myriad of problems--military, civil, industrial, commercial, or whatever. Oddly enough, the same thing is true to a lesser extent and in varying degrees in other countries around the world. So the prospect of applying our know-how, expertise and proprietary materials and processes to the solution of foreign country problems becomes remote. And while it may appear that we are giving away our know-how for a small return, we always manage to come up with solutions that require purchasing a high percentage of our products that are unavailable elsewhere.

So the problem we face is in applying the principle of technology transfer to the development of business opportunities in foreign countries. Where it is a military product with a friendly nation, there are road maps which can be followed and, as the gentlemen on the panel who preceded me have indicated, there are a number of unmarked hazards and detours to be overcome but generally the problems can be worked out. Where it is a high technology effort with a non-aligned or controlled economy nation one must approach the problem much like the porcupines making love--very carefully.

One area where progress could be made in promoting trade where the benefits would outweigh the possible

compromise of security is consideration of the releasability of technological fall-outs from military programs at the time the original analysis of classification is being made and similarly at each subsequent review of the DD 254. By this I mean that a determination be made on whether a commercial version of a military product can be released and to what countries. Further, that a similar determination be made on which of the technologies required to meet performance objectives require control over their release.

To illustrate the point let's look at the classification of a strap-down inertial navigation system. As you know there have been a great many papers published on the principles of operation and the advantages of strap-down navigation systems and as a result commercial airlines around the world are looking at them critically as the most attractive system for their next generation aircraft. The DD 254 for a military funded development program for such a system reads as follows:

"All aspects of the work under this contract are UNCLASSIFIED except for the following: ..." and then the DD 254 lists a series of accuracy parameters such as position, velocity and attitude accuracy, which it says are "CONFIDENTIAL" but with the following note: "The above indicated classification applies only if the gyros' random and/or compensated drift rate is less than (blank) o/hr RMS per axis and/or the system's position error is less than (blank) mi/hr CEP. Now...can you imagine the problem of a potential commercial customer asking the very obvious question, "How accurate is your system?" The obvious answer, of course, would be, "Adequate for your requirements unless they are very stringent in which case I can't tell you because its classified."

We have been approached by the French who are interested in obtaining a license for producing strap-down systems for their aircraft because they have concluded that we are sufficiently ahead of them in development that it would be economically more attractive to buy the know-how than to develop it themselves. When they reviewed with us the development work they have been doing, there was no question in our minds that they were on the right track and would wind up with a good system. However, in light of the words of the DD 254 they could conceivably complete their development long before we could unscramble the problem of whether we can tell them how accurate the system is.

Let me tell you of another situation where a technological fall-out from a military development offers a potential means for combating a natural disaster. We have been doing some rather extensive work with the U.S. Geological Survey, Center for Earthquake Research, with a device called a Tiltmeter. In principle the Tiltmeter sensor is simply the ancient bubble or spirit level, in which the position of the bubble or void in a body of fluid is used to indicate the attitude of the fluid container with respect to gravity. It has been adapted by the addition of electrical circuits to permit indication of bubble readings into automatic control loops. Sounds simple enough, but the clincher is the accuracy and sensitivity of the device. To impress people with the significance of its capabilities we have printed a brochure which says, "If the whole USA should tilt so that the East Coast rose by an amount equal to the diameter of a U.S. half-dollar we can measure the angle of tilt on the West Coast." That incidentally is an angle of 5×10^{-7} degrees or a 5 with 6 zeros in front of it. By observing the behavior of the tiltmeter mounted on a 13-ton block of granite (which incidentally I can tilt sufficiently with my hand for the meter to respond) we have observed a correlation between the build-up of earth tilt and the subsequent occurrence of an earthquake. After the quake which the tiltmeter also records very accurately as a seismometer the earth tilt is restored. Unfortunately the correlation is not 100%, however a group of Russian scientists have been doing some interesting research which indicates that there is also a correlation between changes in the waveform of primary and secondary shock waves from small seismic disturbances and the occurrence of severe earthquakes. It appears that a joint research project with the USSR to use the tiltmeter (which records both phenomena) to predict earthquakes so that people may take precautionary measures would make a lot of sense. There is even hope that a means may be available for preventing earthquakes. Scientists experimenting with geothermal energy, where they pump water deep into the earth to create super-heated steam for power generation, have found that the process creates low magnitude earthquakes which appear to relieve the build-up of pressures that tend to lead to higher magnitude earthquakes. Installing geothermal systems along faults such as the San Andreas fault could be the answer.

Sounds beautiful, doesn't it? Now comes the hooker. The tiltmeter originated as a device for aligning the navigation system in a strategic missile; it is also used in the calibration of

inertial instruments to provide a very high degree of accuracy in military weapon systems. When you consider the fact that export approval on the technology required to build a modern truck factory in the USSR was held up for months and months because someone was concerned that the Russians would use the factory to produce military trucks, the probability of obtaining approval to release detail data on tiltmeters for a joint research project, or to sell devices to the USSR is extremely low. I guess for the present, the Soviet scientists will have to struggle along with their conventional tiltmeters which consist of two six-foot long pools of mercury installed in a precisely temperature-controlled vault in place of a one-inch diameter bubble level.

Now, I realize that I have selected a couple of "way-out" examples to overdramatize the problem and I am probably guilty of suggesting a utopian solution because it would greatly simplify my job of trying to get a better return on the technology that the government and my company have invested in. It also is possible that some of you are working the problem and it obviously has an element of passing the buck to you classification managers. However, on the other side of the coin I think it has been clearly demonstrated that advanced or long-range planning is a necessary discipline for doing anything well. The defense establishment--both government and industry--do it extensively. We plan our research and development programs to provide solutions to defense requirements projected many years into the future. I am suggesting that consideration be given to introducing an element of long-range planning into the classification system to address the problem of the releasability of high technology data and products for both military and commercial applications in foreign countries. Who knows, it might make the processing of applications for export licenses sufficiently predictable to permit accurate forecasting of foreign sales.

PRESENTATION BY MR. NEHLS

The keen interest and economic considerations of American industry in foreign trade have been dramatically brought to your attention this morning by Messrs. Brown and Silver. Our national government supports industry's efforts to increase their overseas sales and, it is the policy of the Department of Defense, as well as other departments and agencies of the Government, to encourage the promotion of foreign export and trade by American companies so long as such activity remains consistent with the national security and foreign policy of the United States.

Within these parameters the United States Government endeavors to assist American industry and friendly foreign governments in the interchange of that classified information which is deemed essential to mutual defense. Note that the key words here are classified information and mutual defense interests. Accepting the premise that only the United States Government can classify United States defense information and accepting the fact that matters of national security and foreign policy are vested solely in the Government, we instantly conclude that the government role in the interchange of classified information is not only of vital importance but essential if there is to be any interchange at all. It is axiomatic that classified information--both ours and that of our allies--requires protection. What vehicle then is used to afford protection to foreign classified information?

Security Agreements

As you might expect protective measures applicable to the international exchange of classified information are based upon security treaties between our Government and friendly foreign states or international organizations. There are two basic types of these agreements: bilateral, those which are between this country and another; and multilateral, those between the United States and several allied powers, or an international treaty organization to which the United States is a signatory member; e.g., NATO, SEATO, or CENTO. It is the United States Department of State, in concert with its foreign counterpart that negotiates these treaties. The most frequently used bilateral agreement is, in security language, a General Security Agreement. General Agreements are fairly standard and refer to mutual defense interests and to the responsibilities of each government for the protection of classified information. Briefly, they agree to: First, give the information received substantially the same protection afforded to it by the releasing government. Second, to use the information only for the purposes for which it was released by the releasing government. Thirdly, to withhold the information from any third government or party unless the approval of the releasing government has been previously obtained. And last, to respect all proprietary rights, patents, copyrights, or trade secrets involved in the information.

General agreements, as the name implies, do not address themselves to the exchange of any specific type or quantity of classified information. Rather, they are meant to provide security assurances, one country with another, for an exchange when the signatory governments decide to do so.

When participating governments intend that the classified military technology exchanged will be utilized within their respective defense industries, General Security Agreements are then strengthened by separate and detailed procedures, referred to as Industrial Security Agreements. Industrial Security Agreements are drafted by the Office of the Deputy Assistant Secretary of Defense (Security Policy), which also participates in their negotiation, and are concluded between the Secretary of Defense and his opposite number in the foreign government. It should be emphasized that they are meant to enlarge upon general agreements and entered into only after general agreements have previously been consummated.

In some isolated instances, the State Department is unable to negotiate a satisfactory General Security Agreement with a foreign government, but the defense ministry of that government is able to offer acceptable guarantees that United States classified information transferred to it will be adequately protected. In such cases, a special agreement is negotiated between the United States Defense Department and the Defense ministry of the foreign government. In actual practice, these agreements are limited in scope and usually involve information of a relatively low degree of sensitivity relating to defense material which has been sold to the foreign country in the furtherance of United States interests abroad.

Each special agreement is tailored to meet the particular security conditions of the foreign government and, at the same time, to satisfy United States security requirements. In contrast, General Security Agreements, and their supplementing Industrial Security Agreements are predicated on the assumption that the foreign government operates a security system which, though differing in detail, is roughly parallel to that of our Government and the United States industrial community.

Bilateral agreements provide the protective framework for the sale of classified military equipment abroad. They also make it possible for foreign governments to purchase certain classified defense material from the United States. And finally, and perhaps most importantly, they enable the United States and the foreign governments to combine their classified technology in the defense interests of their respective countries.

Multilateral Security Agreements, on the other hand, are concerned with protecting classified information contributed by the United States and

other nations as participants of international treaty organizations. The internal instructions of each of these treaty organizations require that each member nation designate an official who is known as that nation's National Security Authority. The National Security Authority is responsible for the security of all treaty organization classified information within his own country. In the United States, the Secretary of Defense has been designated as the National Security Authority for NATO, SEATO, and CENTO. This designation except for a few particulars, has been delegated to the Deputy Assistant Secretary of Defense (Security Policy) for implementation within the United States.

Classification Guidance

A few minutes ago I spoke of Industrial Security Agreements which amplify existing General Agreements. All Industrial Security Agreements consummated by the United States are in consonance with the procedures of the Industrial Security Manual for Safeguarding Classified Information and it is in these agreements that we find the theme of classification guidance.

Here we find a clause stating substantially that each government in the process of negotiating a classified contract within the other country, and every contractor in receipt of a government defense contract who is in the process of negotiating a classified subcontract within the other country, shall incorporate in that contract, request for proposal or subcontract document an appropriate security requirements clause. The appropriate activity of the contracting government shall furnish the designated agency of the government responsible for security administrative measures concerning the contract and the contractor or subcontractor with the security classification guidance pertaining to each classified element related to the contract. This guidance should be in the form of a Security Requirements Check List or, if necessary, written detailed special instructions. The objective is to identify that classified information which is furnished by the contracting country or which is generated pursuant to the contract and to assign to such information the proper security classification. A reproducible copy of the classified contract containing the security requirements clause and appended security guidance will be submitted to the appropriate government agency which is responsible for administering contract security measures. Within the United States this would be the Defense Contract Administration Services Region (DCASR) having geographical jurisdiction of the performing contractor. These procedures have the familiar ring and are certainly

comparable to the Armed Services Procurement Regulation and the Contract Security Classification Specification (DD Form 254) which are all too familiar to our domestic operations. To this point we have been considering security guidance as it would emanate from the foreign interests awarding a prime contract. What happens when you--the prime contractor--desires to subcontract a portion of your foreign classified prime contract. Recalling that third countries cannot be involved we will restrict our considerations within our own borders. You--the prime contractor--will develop the security classification guidance for your subcontract in the same manner using the DD Form 254 you would if the original contract were of domestic origin. The DD Form 254 which you propose for the subcontract will be sent to your cognizant security office for further transmittal to the foreign government concerned for its approval and authenticating signature.

From this criteria we quickly deduce that the provisions for security classification guidance parallel in the international environment, the provisions applicable on the domestic scene. The format conveying the guidance may differ, and the familiar DD Form 254, Contract Security Classification Specification may not be used. However, there is a growing acceptance by foreign governments to use a check list format similar to our DD Form 254. Canada is a case in point.

NATO Classification Management Program

And turning again to our multilateral arrangements it is interesting to note that NATO has currently under study a full blown classification management program. In fact, the United States delegation to the NATO Security Committee submitted a Defense developed proposal to that Committee to incorporate within NATO, a classification management program similar to that which is in use throughout the Department of Defense and which is based on the provisions of Executive Order 11652. This proposal was circulated within the member nations of NATO by the Director, NATO Office of Security on September 5, 1972.

A Working Group was formed composed of members of the NATO Security Committee. These representatives met in Brussels during October 29 - 31, 1973 to study the United States proposal. The Working Group voted unanimously to submit the proposal to the full Committee with some minor adjustments.

On November 6, 1973, the Working Group's report was circulated to all members of the NATO Security

Committee with the request that members submit their comments on the report by January 25, 1974. These comments were considered at the March 1974 meeting of the NATO Security Committee. Coordination between member nations on this matter is continuing.

If adopted, this proposal will provide, for the first time, an automatic downgrading and declassification system within NATO.

Conclusion

The problems involved in achieving a proper balance between security considerations and increased international trade may not be simple, but they are far from insurmountable. Mutual understanding and help between industry and government is the key to achieving the maximum benefit for all concerned.

General Security Agreement supplemented by their companion specific Industrial Security Agreements establish the requirements among which is classification guidance. Knowing all this what do you do--as an American contractor--to obtain the security guidelines necessary to protect the other nation's classified information when it is entrusted to you. It appears to me that our domestic classified procurement procedures are analogous. Knowing that the government procuring activity, or prime contractor, has the issuing responsibility, the subject of classification guidance should be discussed in the earliest stages of negotiation. Agreement between all parties concerned as to what is classified and when, will preclude agonizing security problems at a later time. Formalized classification guidance should--in all cases--be part and parcel of the final contractual document.

As in many walks of life these days getting done what should be done is not always as easy as it sounds. To assist you with classification management problems involving foreign governments the Defense Contract Administration Services Region offices of Industrial Security are there to help. In the Industrial Security Staff Specialist (Classification Management) you have an advisor and counselor who also has a channel open to him to communicate, on a government-to-government basis, with the foreign entity to assist you to get the classification guidance necessary to provide the requisite protection. Make your needs known to these security professionals for only then are they in a position to help you.

Working together, industry and government we are able to pursue the basic national policy of expanded trade with those countries with which we

have diplomatic or trade relations, while at the same time avoiding risks to our national security.

On behalf of all Defense Supply Agency Industrial Security personnel nationwide, I would like to express my appreciation for this opportunity of participating in this seminar with you.

Thank you very much.

QUESTIONS AND ANSWERS

MR. RICHARDSON: I'd like to address my questions to Mr. Silver.

I've heard part of your presentation before, and I find it very interesting, very comprehensive, and very much by the book, which is the way we have to live. I understand--and you may know--that there is a move to remove the requirement to check with the Contracting Officer and get specific written authority before submitting an application for an export license.

Have you heard this? Do you understand that this is afoot?

MR. SILVER: I heard that it was afoot over a year ago, and I was expectantly awaiting its issue. At this point, I have almost lost faith that it's going to be issued.

MR. RICHARDSON: The other comment I'd like to make on your presentation is to ask whether or not you've submitted this through NSIA recommendations as a position paper through NSIA to CASSIA or to John Sipes?

MR. SILVER: No, I have not.

MR. RICHARDSON: I think it would be a good subject for it, because there are so many things involved in it. There are so many regulations that have to be changed, three that I know of in your recommendations that are very valid points, and I think it really should be submitted through Hughes' membership in ELA and AIA. It would be a good place to get started, and I recommend it.

MR. SILVER: Thank you. I intend to do that. I think that the program even cuts a little deeper. All references in the Industrial Security Manual that reflect on international operations should be coordinated so that they all support the same overall policy.

If you read the section on employees with Overseas Security Eligibility determinations, you will find a great inconsistency with regulations that govern

the dealings of U.S. stationed employees making overseas visits.

MR. CORREIA: Are there any other questions? Yes.

MR. KOETHER: Fred Koether, ARPA. I'd like to clarify a point with Ed Silver. You said that a Contracting Officer makes foreign disclosure policies. I don't believe that's a proper statement.

He may make foreign disclosure decisions, but the policy is made by the national disclosure policy committee.

MR. SILVER: My point is that if I have an "X" weapon and want to get a document that describes that weapon cleared for release, say, to the Swedish Government, and I ask for permission to publish and distribute that document, and I receive a denial ...

MR. KOETHER: But that's not a policy. He makes a decision of either disclosure or...

MR. SILVER: In any case, the result is the same.

MR. KOETHER: Yes, but...

MR. CORREIA: Well, I think what Fred is bringing out, Ed, is the fact that the Contracting Officer is preventing you from making any disclosure to a foreign government. You are stopped there. That's really what you're saying.

MR. SILVER: I think we're in agreement. The results would be the same. I realize that. The point I'm trying to emphasize is that the Contracting Officer ends up with more power than what it was envisioned he would have when the regulation was written.

MR. CORREIA: Any other questions? Yes.

MR. FLORENCE: Bill Florence, Security Consultant.

In my contacts around Washington, D.C., I liaised quite closely with some of the Congressional Committees interested in developing legislation to sort of pre-empt some of this other classification information Mr. Brown mentioned. I have a couple of questions of Mr. Brown. I believe his answer should be of interest to everyone here.

I have in mind, Mr. Brown, the suggestion that you made that there should be more of a formal establishment of long-range planning programs involving the research and development of objectives, and

along with this suggestion you're making, I'm hearing a great deal across the country in my contacts these days of objections to the long time practice of the Department of Defense of there being classifications of technical information on a program-by-program basis resulting in program officers, program directors, exercising necessarily a proprietary interest in information involving the programs, and applying what you might call a parochial-type classification decision on technical information which really is very common, and the suggestions that I have heard that are being made recently is that the Department of Defense should reorient itself in this matter of classifying technical information and classify technical information and technology on the basis of the value of the information from a technological standpoint, rather than a program-by-program basis.

So, I wonder if you would care to comment on the relative merits of a development of policy for a technological classification where classification is always required, rather than program-by-program classification, or to eliminate some of these contradictions that you referred to in these two programs?

MR. BROWN: I'm not sure I completely understand what you're saying.

I think you're suggesting that there be a program on a DD 254 on a class of technology, rather than on a program and the technology contained therein. Is that what you're saying?

MR. FLORENCE: The point I'm making was the Department of Defense policy, their classifying to determine the need for classification of technology so that then DD Forms 254 for particular contract work or program work would reflect a requirement or the absence of a requirement for classification of the technical information involved, rather than for a decision to be made on a program-by-program basis.

For example, in this level-type information technology, we're talking about accuracy, you would have a classification determination from the standpoint of the development of technology to be applied regardless of the program the information it was involved in, this is the question.

MR. BROWN: I think I may have misled you. The things that I was discussing were high technology items that are not classified, but are still within the ITAR regulations as far as requiring export approval, and because of the fact that some are developed under a military program or military-related program, it goes through the

same coordination cycle as classified material does, and typically, the service involved will turn it down because of their knowledge of its having been developed for a military application just in principle, and I'm talking about commercial applications of these things.

So, again, I'm afraid I don't understand your question well enough to answer whether things be done on a technology basis. I think that would be difficult to administer because you would have to go to the Presidential Scientific Advisory Board, something like that, to make a determination on technology per se, and a lot of these things are just know-how, taking fundamental principles and applying them to a day-to-day solution of a problem, but with military origin and from a military program where you're tied into the ITAR and have to get export approval through the Office of Munitions Control.

MR. FLORENCE: Thank you. May I ask one question of Mr. Silver?

I believe Mr. Silver's comments were directed even perhaps more specifically to restrictions on this export of information stemming from the existence of classification assignments.

In relation to the proposed regulation that committees of Congress are working on that I alluded to in the beginning, would you care to comment on this, whether the establishment of a hard limitation of, say, perhaps, three years duration of classification for strictly technical information as such would tend to eliminate these problems that you have expressed so strongly here this morning?

Would there be a time limit on the classifications warranted for your technical information that would assist you in furthering the export trade you're talking about?

MR. SILVER: Starting in reverse order, I guess I would have to say yes, it would help, but to generalize like that I think is very difficult.

To generalize and say that all technical data should be declassified after three years is an oversimplification.

MR. FLORENCE: Well, there's no program that I know of anywhere in the country that all technical data would be declassified after three years with no exceptions.

There would be exceptions allowed.

MR. BROWN: Thinking a little further about your comment or your question, in effect, the ITAR controls technology per se by what it classifies as arms, and, for example, commercial navigation equipped with anything related to that is under ITAR and has to get export approval.

MR. CORREIA: I want to thank the panel that I had here, Mr. Silver and Mr. Brown and Mr. Nehla. I think they did an excellent job and I hope it was informative to you.

A LOOK AT THE ARMED SERVICE PROCUREMENT
REGULATION

BY
CAPTAIN (USN) EDGAR C. CHAPMAN, JR. (Retired)
Manager, Contract Administration
Teledyne Ryan Aeronautical

The first thing I would like to do is apologize for making you delay your luncheon, but I really do appreciate this opportunity to come on now.

I arrived in time to hear some of the panel that was just on and I gather that like most members of the procurement community, you all have problems. Maybe in the course of my discussion of what the armed services procurement regulation ASPR is all about, and how it gets written you will find a key to help solve some of your problems.

Let me describe ASPR first and give you a feel for its magnitude. The purpose of ASPR is to provide uniform policies and procedures throughout the Department of Defense. In other words, it tells not only what to do, but how to do it. In theory, it is not supposed to be further implemented down by the various Services and Agencies of the Department of Defense. It should stand on its own two feet. There are, of course, exceptions to that, but, really, Departmental and Agency implementation should only tell who in an organization does something, not what they are to do.

ASPR consists of twenty-six sections, which I guess you'd normally relate to a chapter in a book, plus fourteen appendices, two manuals and five supplements. Altogether they total well over three thousand pages. Fifty-four thousand copies of ASPR are printed by the Government Printing Office. About half of these go to DoD purchasing offices, and the rest go to libraries, contractors, foreign governments, and so forth.

ASPR covers almost every facet of procurement that you can think about. Not only the contracting side--although it is aimed primarily at the

Contracting Officer, telling him what he has to do or what he has to get into a contract--ASPR also has a lot of other parts.

I started to say earlier that when you put a requirement into ASPR, it often makes the "experts" in DoD unhappy, because now the "system" takes over and drives what goes into the regulation. Often the technical experts in a field like construction or transportation or patents or whatever lose a great deal of the control that they previously had before. But I can also say that it's a very fine way to get things done.

I can remember one case. I won't tell you what the subject area was, but one of the officials in the office of the Secretary of Defense (Controller) put out a regulation on how to do something, and it was a very important area. Two years later, not one of the services had done a thing, and in total frustration, the official came to the ASPR committee and asked that we take their requirement and put it into ASPR. I fought, because I really didn't think it should be made a responsibility of the contracting officer. Ultimately, I lost, because my boss, the Assistant Secretary of Defense, I&L, said we would do it. And we did. We revised ASPR and now, about three years later, it's a very viable program. The requirements are getting into contracts because the contracting officers, and the standard clauses in ASPR, are putting it into the contracts, and now the job is getting done.

So there is a way to get things done. But ASPR covers, as I said, just about every facet of procurement, the kind of basic things like small purchases, formal advertising and negotiation. It also covers specialized areas such as patents, data, copyrights, bonds, insurance, taxes, industrial relations, and etc., etc., etc.

The one thing it doesn't cover very well, incidentally, is industrial security. In fact, I looked it up yesterday. I couldn't remember a case during the four years that I chaired the committee. And I looked at the current ASPR case list. I couldn't find anything on industrial security. I looked at ASPR and found virtually nothing on industrial security.

Anyway, to summarize it all, I would say that ASPR is often referred to as the Bible for procurement. I can tell you, particularly since I have been in industry and have looked at it from "the other side of the table," that ASPR is a Bible to the contracting community. They do follow it. In fact, if all the good church members followed the Bible as well as the contracting community follows

ASPR, I expect there would be a lot more people in church every Sunday.

ASPR goes back a long way. It goes back to right after World War II. Before World War II, almost all contracting was done on a formally advertised basis. That's where bids are submitted by contractors. They're opened publicly and read and, generally speaking, the low bidder gets the job.

During World War II, of course, a lot of that went down the drain and they negotiated a lot of contracts. In 1947, after the War, the Armed Services Procurement Act authorized the continuation of the use of negotiated contracts. At that time President Truman wrote to then Secretary of Defense Forrestal, emphasizing that this bill gave unprecedented freedom to make procurements in peace time, expressing his concern and saying that, "I want you to put out regulations which will control the activity of your contracting types to make sure that they do a good businesslike job." From that evolved ASPR. That was in 1947. The first publication that appeared was around 1950. So nearly twenty-four years ago, ASPR started. The ASPR committee system, which I will try to describe, has remained virtually unchanged over those full twenty-four years. That doesn't mean it's a perfect system. It's a long way from being perfect. It's only that nobody has been able to invent a better wheel. It's been looked at. It's been cussed and discussed and everything else. When they get all done, they perpetuate the existing system, because it is pretty good.

Let me first describe the ASPR committee, which is responsible for writing ASPR. It is comprised of nine members and an Executive Secretary. The chairman comes from the office of the Secretary of Defense and there are two members each from the Army, Navy, Air Force and Defense Supply Agency.

One of those two members from the military departments and DSA is a lawyer; one is a contracting specialist. They are all required to have extensive procurement experience and at least three years of very recent experience in order to go to the committee.

In my time there, the civil service members were all GS 15's, except one 16, and the military were all Navy captains or colonels, with only one exception to that.

They are also required to serve, once they go to the committee, a minimum of two years and a maximum of four. We don't want to rotate the members every day, because there's too much continuity

required. At the same time, about four years is as long as a member can do something like that and not become a bureaucrat, and we really try not to have bureaucrats setting the policy. What DoD wants is people who have just been sitting at the table negotiating live contracts and putting their experience to work.

As I said, ASPR is some three thousand pages long. A lot of that came about because it is now full of administrative or "how to do" requirements as well as policy. This very significant and explosive development took place in 1963, when two different things happened. First was a reduction in implementation program in which they tried to codify all of the military department regulations.

They got together, wrote one regulation and they did away with some six thousand pages of Army, Navy and Air Force implementation. So it was a pretty good effort. ASPR grew by about 800 pages--but about 3,000 pages of departmental regulations were eliminated.

At the same time under Project 63 where the contract administration services were set up, under the ASPR committee they had a Contract Administration Panel. It was a mini-ASPR committee and their job was to put into the regulation all of the things necessary to provide for uniform contract administration. Included were such mundane things as how to number contracts. You can't believe how important that becomes when you have a whole lot of offices, flowing into one office, documents which they have to administer.

You have to be able to look in the same place in the contract for the same thing: The schedule, the general provisions, the special provisions and all the good things that make up a contract.

The end product of the ASPR committee is recommended revisions or additions to ASPR. All these recommended additions and revisions are given final approval either by the Assistant Secretary of Defense for Installation and Logistics for major policy--and, believe me, he personally gets into it. Incidentally, on anything that's major policy, I can also assure you that the Assistant Secretary of the service involved, Army, Navy, Air Force, would be personally involved and the director of DSA.

All other revisions and additions which are not considered to be major policy are approved by the Deputy Assistant Secretary of Defense for Procurement.

The work load of the ASPR committee runs something like this: There are about a hundred and fifty to two hundred new "cases" which are opened each year.

About fifty percent of these come from within the Department of Defense. If somebody in the Department of Defense thinks they've got a problem, it flows up through the chain of command to the ASPR committee and is reviewed. In addition to that, there are many Federal laws to be implemented; ASBCA and Court of Claims decisions to be effected or countereffected. Other Federal agencies, and I think particularly of the Small Business Administration, Department of Labor, Equal Opportunity provisions, and the General Accounting Office and their audits of procurement process all recommendations which are taken under consideration. And not last and certainly not least are Industry Associations recommendations.

There are some eighteen industry associations that the ASPR committee interphases with; such outfits as Aeronautical Industry Association, Electronics Industry, Shipbuilders Council Automobile Manufacturers Association, and the Federal Executives Institute. Altogether eighteen rather significant groups that represent the general--the total spectrum of industry in the United States.

The basic work force of the ASPR committee is its subcommittees. At any point in time, there would probably be an average of thirty-five subcommittees working on ASPR cases. Their members would generally come from Washington, D.C. However, they would come in from operating activities all over the United States at times.

A subcommittee can have as few as three or as many as a dozen members. I think of one--if you're familiar with the cost principles of ASPR--that's the part that says what costs are unallowable as charges to Defense contracts.

On that subcommittee, which was quite an active one, we not only had all of the military services and DSA represented, but also the Defense Contract Audit Agency plus NASA, Atomic Energy Commission and the General Services Administration.

I counted at one point in time this and we had a membership of our subcommittees of a hundred and ninety good people. And I do mean good people, because I never ceased to be amazed at the quality of the people that worked on our problems.

They were universally outstanding.

A typical ASPR case, and this is awfully hard to define, is a very lengthy, a very thorough process.

A problem is presented to the committee and the committee takes a look at it and decides yes, it at least needs to be looked at. It doesn't say we have a problem. It says we need to examine whether there is one. This "problem" is assigned to a subcommittee. The subcommittee is given thirty days to review it, identify any problems that exist, and recommend the solutions, and propose a draft revision to ASPR.

At the end of thirty days their report is circulated throughout the Department of Defense. About a hundred and thirty copies are spread throughout the OSD headquarters, the Army, Navy, Air Force, DSA, Defense Audit Agency, and so forth. They are given three weeks to review this and then report back to their ASPR committee member what they think of the case. Incidentally, these hundred and thirty copies of the subcommittee report go to headquarters level personnel and to the operating negotiators in the field, so that the ASPR committee will hopefully, hopefully, get a broad spectrum of opinion on whether there is a problem and whether the subcommittee's proposed solution is workable or necessary.

At the end of the three weeks, the ASPR committee takes its first cut at the proposed problem solution. They review it, decide where they want to go from there. Incidentally, if it's reached that far, there probably is a problem, and probably something is going to get printed.

At that point in time, what the ASPR committee has then developed out of the subcommittee report is circulated for two months. It goes to four other Federal agencies: NASA, AEC, General Services Administration and the General Accounting Office, and, in addition, it goes to the eighteen industry associations that I mentioned earlier.

At the end of that two months, hopefully, they have quite a number of comments back and all of these comments--and I've seen them in a single copy stack 12 inches high--on a very controversial case. Sometime they don't get too much interest, and, obviously, they don't get too much response. At the end of the two months all comments received are furnished to the original subcommittee. It's their job to analyze all the comments; either accept them and work them into a proposed revision or reject them and tell the committee why.

This report, quite a lengthy thing usually, is returned to the ASPR committee; is circulated throughout the Department of Defense for another three weeks for comments. Then the ASPR committee takes a final cut, and, at the end of that time, they vote. I'll go through it again. A case is given to a subcommittee. Their report is coordinated throughout DoD for three weeks. The ASPR committee considers it, decides what they think they might want to do. It's then coordinated with other Government agencies and industry. The subcommittee takes another cut at it. The ASPR committee takes another cut at it and it is then ready to be voted on as to whether it goes into ASPR or not.

At that point in time, a majority vote rules. There are five votes on the committee, one for each military service, DSA, and the OSD staff. As I said, so majority vote rules, except in one set of circumstances, and that is if any one of the services or OSD feels very strongly that they cannot live with the majority vote of the committee. They then have a right to make it what is called a "secretarial issue." A secretarial issue can only be made by the Assistant Secretary, (I&L) of one of the services, the director of DSA, or one of the Deputy Secretaries of Defense. They personally have to sign a memorandum to the Assistant Secretary of Defense (I&L), stating their objections. At that point in time, the Assistant Secretary of Defense (I&L), calls a meeting of these gentlemen with whom he coordinates and it's cussed and discussed again. Usually, it's the chairman of the ASPR committee's job to present both sides of the case, and then the Assistant Secretary of Defense makes a final decision.

Whatever he says then becomes law, and I guess that's really not a bad description, because, in fact, that's just really about what it amounts to.

I think you can see the ASPR committee process is very, very thorough. Does that mean it doesn't make mistakes? Heck, no. They've made lots of mistakes and they come back to haunt you if you were the guy that put it in there originally,

Every case has had, in the aggregate, hundreds of people looking at the proposed revision, hopefully making comments, and those comments I can assure you were always very heavily considered. Very bluntly, I'll also tell you however that our major problem in the ASPR committee was lack of input. We put out a hundred and thirty copies to

the Department of Defense and you were darn lucky if you got six replies. That's very frustrating since the whole name of the game is to get operating impact into what was being done.

The same thing was true of industry associations. Associations tend to put forth only a single point of view and it usually lacks hard facts.

We always found when I had the ASPR committee that if we could talk to individual company representatives face to face and without any possible retribution from an irate contracting officer, we could get a lot better story than we often got from industry associations. Notwithstanding the problems, it's a very good process and I think that probably is why the committee has withstood the test of time. With all these people participating, it's pretty hard to shoot down the final product, and I think it is also probably why ASPR, over the years, has been called the "model" Federal regulation, and why a number of agencies have copied this method of regulation development. This includes the General Services Administration in their development of the Federal Procurement Regulation and the new Cost Accounting Standards Board, and the way that they develop cost accounting standards. There are many examples of where the ASPR system has been copied, and personally think rightfully so, as I look back on my four years as chairman of the ASPR committee. Now I'll entertain any questions that anybody might have and see if I can answer them.

QUESTIONS AND ANSWERS

MR. HOYLE: Jim Hoyle, Lance Project Outfits, Atomic Missile Command.

I have one question that hit me in your last statement. If the ASPR is copied and may be fairly closely with some of the other services of Government agencies, why not have one regulation and make it composite?

CAPTAIN CHAPMAN: As you know, the NASA procurement regulation is almost a verbatim copy. There's a couple of things they didn't like and didn't put in there, but it's so close you can't hardly tell it. The Federal procurement regulation is a great deal smaller, but where they cover the same subject matter, they're identical. AEC is probably pretty much the same way. I see no really good reason why we can't and shouldn't have uniform policy, but, again, remember that I said that ASPR not only tells you what to do but how to do it. For example, ASPR has become a procedural document that divides up the world between the PCO and the ACO. However, none of the other Federal agencies have an organization like DCAS. In other words to have a single

publication, you'd have to have something else to fill that procedural gap. I do think that probably we're going to get to a single top level policy regulation if the Office of Federal Procurement Policy ever gets established.

MR. RICHARDSON: Dean Richardson, Texas Instruments.

Do you have, or can you tell us if the ASPR is based on legislation or Executive Order?

CAPTAIN CHAPMAN: Well, the basis of ASPR is legislation. I ought to refer you to my old lawyer over here, Murray Marker. Murray, am I right in saying that it has a basis in legislation in the Armed Services Procurement Act?

MR. MARKER: Yes, it stems from the Armed Services Procurement Act.

CAPTAIN CHAPMAN: Although the Regulation is bottomed on law, a great many of the policies that are in it are purely developed by the people in the Department of Defense. They have no basis in law.

MR. RICHARDSON: Well, the reason I asked the question, if I can go on, is if it is based on law, then it's really out of the Executive Branch. Okay?

Now, the next question is if we have conflicts, and some people in interpretation think there are conflicts--it just depends on who you happen to be dealing with--between the industrial security manual and the ASPR, which is to supercede which?

CAPTAIN CHAPMAN: Well, I guess it all comes down ultimately to how does a manual become involved? Remember that a contract is only what's between the front and back page of a contract. ASPR itself doesn't really govern a contract so much as it does the people in the Government who write contracts.

ASPR, as a total regulation is not incorporated in any contract. What you do is you get down to all the elements that make up a contract, the schedule, the specification for what is being bought, and all of the clauses that are put into it, including many which are standard, required clauses or optional clauses out of ASPR. If there's a conflict within a contract, the contract provides for that, too, because each one has an order of precedence clause which says what part of the contract take precedence. I don't think that discrepancies between various parts of a contract is fatal.

MR. RICHARDSON: Well, it can be fatal to a contractor. It can be fatal to a contractor cost-wise if the ASPR as determined by our contract administrators says this and they come to me and they say, "Okay, let's be sure that we're following the rules according to the ASPR," and how is this interpreted by the Government when they put this into contracts, and they say, "This is fine."

Now, my interpretation of this security clause in the ASPR is this. However, when that gets into the DCASR QA, and I'm not blaming the DCASR, it could just as easily be the PCO, he may read it a little differently and he can interpret it a little differently, so what he can really say to me is, "My ASPR is based on law. Yours is based on Executive Order; therefore, what I say in here takes precedence over your industrial security manual, which is a DoD directive."

No question, just a comment.

CAPTAIN CHAPMAN: Well, yes, again, I guess I'd have to go back instead of trying to say what ASPR says--and particularly in a case like this--I'd have to go back to what the contract says, and that's what the contract administrator better be interpreting. No two people read clauses the same way. That's for sure. I've got a contest going with our DCAS right now about what a clause says. I think I know what it says and they think they know what it says and, obviously, one of us is wrong, and even though I think I'm right, I think I'm going to lose. (Laughter.)

The ultimate place to get a decision, particularly when it relates to cost, is, of course, the Armed Services Board of Contract Appeals whose job it is to interpret the contract and what the contractor's obligations are when there is a dispute between the Government and the contractor. Of course this takes time and costs a heck of a lot. That's why I think I think it's a lousy way to go, but sometimes it's the only way you can get a decision that's meaningful. Yes, ma'am.

MS. ALEXANDER: Colleen Alexander, Convair Libraries.

As an acquisitions librarian, we are required to purchase all of the ASPR for the entire company. About how often do you anticipate basics will be--come out on this, or will they be continued on a revision--

CAPTAIN CHAPMAN: No, I noticed in the last defense procurement circular that the ASPR committee has finally decided to print, totally reprint and you will pay for ASPR each year. If you have the 1973 edition though, you will be entitled to a 1974 edition without additional cost.

MR. CHELIUS: I'm advised that in the near future the DoD safety manual for contractor's facilities will be incorporated into ASPR, or at least I've heard rumors to this effect. Based upon that, would you then say that there might be a possibility that the industrial security manual would be incorporated into the ASPR?

CAPTAIN CHAPMAN: Again, I would have to say that before the industrial security manual would be incorporated, it would be because those in OSD who are responsible for this area want it there and request that it be there. The ASPR committee isn't going to go out and pull it in.

MR. CHELIUS: Thank you very much. Other questions from the floor, please. Are there other questions from the floor?

CAPTAIN CHAPMAN: Thank you very much.

MR. CHELIUS: Thank you very much for appearing. I think we've all appreciated the interchange of discussion.

TRENDS & DEVELOPMENTS IN INDUSTRIAL SECURITY

BY

R. E. GREEN

Chief, Programs and Systems Division
Office of Industrial Security, CAS

It is always an honor and a pleasure to attend a National Classification Management Society Seminar (NCMS) to meet with old and new friends and to share for this brief time our mutual concern, achievements and problems in the oft-times perplexing business of Classification Management. As some of you are aware, I have, in the past, addressed this society as a representative of the Department of the Navy, and I am grateful for those opportunities. This year, however, I wear a different coat, but cut from the same cloth; our mutual and abiding dedication to the proper management of classified information wherever it is generated or held.

I consider it an additional privilege this year to represent the Chief, Office of Industrial Security, Defense Supply Agency, more familiarly known to you as DCAS. Colonel Clark, whose staff I joined last November, has asked me to convey to the society his regret that other commitments made it impossible for him to be with you today, to offer congratulations on your 10th anniversary, and to assure you that, as you launch the next decade of progress for the NCMS, you have the best wishes of the entire staff of the Office of Industrial Security. We thank you, individually and collectively, for your past contribu-

tions to the Defense Industrial Security Program and we look forward to continued progress together. I would like to take a moment of your time to introduce the other members of the DCAS family who are in attendance and participating in your program. From the headquarters staff, Mr. Rae Nehls, Field Management Division, whom you heard earlier today as a member of the International Security Panel. From our academic branch, Major John O'Leary, USAF, Assistant Commandant, Defense Industrial Security Institute at Richmond, Virginia who will give you a rundown on the new Information Security Management Course. Last, but by no means least, the guys and gals who can be of most immediate help to you, the Classification Management (CM) Specialists from some of our DCAS Regions: Bob Coon--Chicago, Betty Mowry--Cleveland, Victor Seyen--Dallas, Lou Sibiga--Detroit, Leo Sharkey--San Francisco, and Charles Micelli--St. Louis. I strongly urge you to establish a first name, running dialogue with them. Only in this way can they fully assist you in resolving CM problems.

As I reviewed some of the achievements of the NCMS, I became aware that, in many ways, the formulation and growth of NCMS parallels that of the Office of Industrial Security. Some of the problems you have experienced over the years, we have shared. Some of the same concern for the future is evident in both organizations. Let's take a moment for some comparisons; a sort of "Did you know?" session. For example, did you know that in the Spring of 1963 while a bunch of your boys were whooping it up at the Weapons Contractors Classification Conference in Kansas City, a bunch of our boys, known as Task Force #12 of Project 60, were doing the same at Cameron Station. I don't know much about Kansas City, but if you can believe that about Cameron Station, you'll believe anything. In your case, the idea of a professional society devoted to security classification management was conceived. In ours, the concept of a single manager for the highly fragmented Industrial Security Program was born and took the form of recommendations to the Secretary of Defense. In the fall of 1963, your resolve created the NCMS as an active group. Only a month earlier the Secretary of Defense had approved the Project 60 recommendation and established a "Pilot Test" for consolidation of Contract Administration Services, including industrial security, in the Philadelphia region. Then, in the Spring of 1964, the NCMS was incorporated and, thereby, legally came into being. Only a few months later, in October, the Secretary of Defense assigned responsibility for administration of a consolidated DoD Industrial Security Program to the Director, Defense Supply Agency; so, in a sense, the OIS, DCAS legally came into being.

And, did you know that even our publications track together? The first revised ISR and ISM under the consolidated concept were issued in March of 1965. The first journal of the NCMS is dated Spring 1965. The nature of our publications is obviously quite different, but it is important to note that your journal has gained wide acceptance as an authoritative, if not the authoritative source of information on the concepts, problems and experiences in administering CM programs in both Government and industry. The ISR and ISM, being directive in nature, have a captive audience; however, I would not care to speculate on whether they are more frequently consulted than your journal. Statistics do support the fact that the ISM is a No. 1 best seller and is frequently out of stock at the Superintendent of Documents, GPO, where it is on public sale.

The important thing is that these publications, yours and ours, are viable documents recording the history and the progress and pointing the way to the future of this most complex security program and its most difficult element, Classification Management.

There are also parallels in our less formal newsletter publications, the CM Bulletin and the Industrial Security Letter and Bulletin.

One of our most commonly shared concerns centers on recognition of CM as the keystone of the DoD security program, and while the society, through both the Government and industry members, was diligently working to establish the CM function as a viable, believable and essential part of the 11 DCAS Regional Offices of Industrial Security. These positions provide a valuable service to the contracting officer and to the contractor as an on-the-scene monitor reviewing the classification guidance furnished by the contracting activity to the contractor and, acting on his own initiative or at the request of the contractor, identifying inconsistencies and potential problem areas and obtaining clarification or resolution from the contracting activity. In related areas, the CM Specialist can be of service in helping to resolve problems in the retention of classified material and in expediting requests for public release of information related to classified contracts. In establishing these positions, DCAS faced the two major problems common wherever there is a CM function; (1) identifying and obtaining the classification guidance applicable to each classified contract and (2) staffing the positions with personnel who were knowledgeable and experienced in CM matters. In the first instance, we had to assemble a base file and

establish a review system, literally by manual means, for many thousands of classified contracts. As an example, one of the 11 DCAS regions alone has a total of 2700 classified contracts under security cognizance. Without detracting from the need for the review and its supporting tickler system, you can appreciate the manpower drain in such a manual operation. Much to our regret, it has precluded, to some extent, the kind of attention we would like to give to substantive and comparative review of classification guidance being given to industry. In the near future the system of indexing and tickling annual review of the DD Form 254 will be mechanized in all Regions, thus relieving the situation somewhat. In this connection, we believe that the need for DCAS to monitor compliance with the annual review requirement has been overtaken by events and could be dispensed with. This would, of course, eliminate the negative reporting requirement which has been an administrative burden on all concerned and in the light of other monitoring capability is, in our opinion, no longer cost effective. We have initiated discussions with Mr. Lieblich's office to that end and hope for an early and favorable decision.

With respect to staffing CM positions, we both face the same problems. Initially, we had little practical experience in CM matters and so we learned by doing and we learned a little on the NCMS and its members for education and consultation. Now that we have experienced personnel in these positions we face an aging workforce that is eligible or nearing eligibility for retirement. As you know, this has also been a matter of serious concern to the society for several years. Within the DCAS organization, 45% of our professional personnel will be eligible for full retirement within the next 5 years. This does not include those who may opt for early retirement under incentive and cost of living annuity increases. With losses of this magnitude will go much of the knowledge and experience we have built up over the years. This situation is common throughout the security community.

Now for a final comparison--a look at our total growth for these first ten years. I don't need to ask "Did you know?" where NCMS stands today. Referring to growth in the more important context of "stature" rather than the common measure of "size," NCMS can be very proud of its place in the security community. Specializing in the most difficult element of the program, CM, you have been foremost in shaping the development of CM programs in both industry and Government. Through your membership and your publications, you have counselled, guided, encouraged and, in a sense, trained many of the CM specialists

currently in the program. Your influence in the field of CM and the stature you have attained are epitomized by your recent contributions to and requested appearances before Congressional committees working on legislative and national policies related to the classification of official information and the availability of such information to the general public. It is an enviable record and a credit to each of your members who made it possible.

Since I am a relative newcomer to the organization, I can speak of DCAS achievements without being accused of immodesty. It is a difficult task to form a new organization as you did in 1963, even with common ideas and purpose. It is infinitely more difficult to mold several existing organizations with their regulations, procedures and personnel into a single cohesive unit working under a single set of groundrules. This task is more complicated when it is accomplished while providing continuous service to the customer, i.e., User Agencies, and maintaining a single face to industry. But that is what DCAS faced and it was done and the thousands of working level problems were solved. We feel that today DCAS (the OIS particularly) functions smoothly and constructively as the middleman between industry and Government in the area of classified procurement. Success is hard to measure, particularly when you try to measure your own, but several things encourage us to believe that we are satisfying our responsibilities effectively and economically. First and foremost, we know of no loss or compromise of classified information in these 10 years which can be attributed directly to a policy or procedural flaw in the Industrial Security Program. Secondly, we have reduced manpower resources from 1534 billets at the time of consolidation to the current 798, while the scope of our functions has greatly increased. This was accomplished primarily by streamlining operations and cutting from the program those cleared facilities and personnel of record whose services were no longer required to meet procurement needs. With respect to increased functions, the basic charter of the Office of Industrial Security has been limited to the protection of classified information in the hands of industry. More recently, that charter has been expanded in several areas which do not involve classified information or the safeguarding of such information in industry. For example, the Defense Industrial Facilities Protection Program, which is designed to encourage industry to develop plans and countermeasures to protect the defense production capability, is now administered by the OIS. We have an interim task of insuring proper safeguards for arms, ammunition, and

explosives in the hands of industry. It appears that this task will be formalized in the next 30 to 60 days. Also, we have been tasked by DoD to present as a part of the DISI curriculum, a course on Information Security Management for DoD Security Managers. You know from the agenda that Major O'Leary will speak on this subject a little later. This again is outside of the scope of the Industrial Security Program.

We like to think that these additional tasks which are not solely within our basic charter are manifestations of confidence in our knowledge of the total security program, and our ability to get the job done with minimum delay and minimum resources. We consider that to be our measure of success.

Finally, I would like to address, from my personal and objective viewpoint, what I consider to be a key factor in the Industrial Security Program, in all of its parts. Over the past ten years, there has evolved from the basic concept, a true joint venture operation between industry and Government to insure that official information is properly classified and safeguarded. Industry's role in both the formulation and implementation of industrial security policy, once minimal, is now substantial and growing. The management philosophy of encouraging and seeking industry's ideas and opinions has never been more evident on the OIS staff than it is today. We recognize and value these inputs and we have a high degree of confidence in industry's ability to take a more active role in designing and implementing security measures for the industrial environment. Those of you who are familiar with the ISM may have recognized in recent changes the greater responsibility being placed on industry, and there are more such changes in the planning stages.

This team concept certainly includes NCMS and other professional societies whose comments and recommendations greatly assist us in arriving at balanced judgments.

In conclusion, from this brief review of our two organizations, you can see that, in the words of a popular Madison Avenue slogan, "We've come a long way, baby." To which you might add words from an old song--"But, baby, you've still got a long way to go!"

We accept that challenge and look forward to another 10 years of parallel growth and development with the NCMS. We know that changing times, standards and needs will force us to keep the program viable. As long as we can meet like this to exchange our views and foster the joint venture concept, the Industrial Security Program will

continue to improve. And, after all, that is precisely why we are here!

Thank you very much.

NEW INFORMATION SECURITY MANAGEMENT COURSE

BY

MAJOR JOHN R. O'LEARY, USAF, Assistant Commandant
Defense Industrial Security Institute

Good afternoon, ladies and gentlemen. On behalf of the staff and faculty at the Industrial Security Institute, it is an honor and privilege to be with you here today to discuss a new information security management course.

Personally, I'm also happy to be here for a number of reasons. It has, first of all, afforded me the opportunity to participate in a truly outstanding seminar. Secondly, it's given me an opportunity to review some old friendships as well as meet many of the friends and alumni of the Institute.

In a lighter vein, the weather here is everything that they've said about it. Southern California is beautiful and those of you who have been in Richmond during July or August know how that can be, and, lastly, certainly in Richmond, you cannot buy any Coors beer.

Historically, speakers always shun away or try to avoid this hour right after lunch because of the drowsiness that sometimes sets in in an audience. However, I think we've got an advantage in this particular subject that we're going to discuss today.

First, because of the advance billing that was received from Mr. Liebling and Mr. VanCook yesterday, it's created a little interest, we hope. Additionally, the course does represent a significant step in the information security management program, and in that line, it's a course that all of us are involved in, interested in, to see, to show, to create this new--and make it a meaningful step forward for all of us.

Additionally, we have departed just a slight bit from the normal presentations that have been given up here. Basically, as Mr. Green described, I'm going to give you just a brief thumbnail sketch of some of the background.

How did this course get started; go into some of the objectives; then Mr. Daigle will get up and give industry's viewpoint of the course. He was in attendance during the pilot course in June,

followed by Mr. Larsen, who will give the Government's standpoint or viewpoint.

Following that, I'll get back up and maybe summarize and give an overall evaluation--a kind of overall evaluation of the course from a standpoint of the Institute, and some of the things that we can look forward to, we can envision in the future of the course becoming.

I think we all agree that the issuance of Executive Order 11652 and the subsequent problems resulting from its implementation pointed out the need for a formal course of classroom training for industry managers, or for security managers and other officials responsible for the proper implementation of this Order. The changes brought about by the Executive Order relating to authority and accountability of classifiers also pointed to formal training as the only logical means of attaining an organized and standardized approach among the various diverse agencies authorized to classify official information in the interests of national security, but the question may remain in some of our minds as to how did this start, when did this start?

We can trace it back to the 13th of April 1973. A memorandum from the Deputy Assistant Secretary for Defense Security Policy was sent to the Departments of the Army, Navy, Air Force, and the Defense Supply Agency.

The purpose of this memorandum was to bring the addressees up to date on the possible development of a course of training in information security management.

The memorandum requested their cooperation in assigning experienced personnel in this field to a Department of Defense task force which was being established to develop the initial materials necessary to establish such course of instruction.

OSD's expressed desire was the establishment of a formal course of classroom training in the information security management covering all facets of the information security program, including classification, downgrading, declassification, marking, safeguarding, personnel security clearances, and other aspects of physical and administrative security.

The memorandum further directed that the course be instructed so as to permit it to be given in two distinct segments. Each segment would be approximately one week in length. The first week covering the classification, downgrade,

declassification aspects that could be made available to security managers in industry.

The training to be supplied was to be designed to meet the needs of the training needs of security specialists who have varying degrees of administrative and managerial responsibility relating to the information security program.

Accordingly, the requested task force was formed and chaired by the office of the Assistant Secretary of Defense Security Policy. It was comprised of representatives from the Army, Navy, Air Force, Defense Supply Agency, and the Institute.

This group met at Cameron Station, Alexandria, Virginia, for three days in June, 1973.

During this period, the initial course requirements and program of instructions was prepared and later approved by OASD. Basically, the program of instruction established that the purpose of the course was to provide a comprehensive understanding and interpretation of the Department of Defense information security program, with particular emphasis on the proper classification of information in the interest of national security, progressive downgrade and declassification action, and safeguards to classified information against unauthorized disclosure.

Further, to assist personnel in implementing and monitoring the industrial security regulation at the individual's command or organizational level, and in satisfying command and supervisory responsibilities for effective compliance with program requirements.

Also established at this task force meeting were the prerequisites for the course as being designed for military and civilian personnel where assigned to or selected for duties involving responsibilities in administering the DoD information security program within the command or organization to which he is assigned. The course is of particular interest to those persons serving as/or selected for security managers' positions within the meaning of DoD Directive 52100.1-R.

The course material is designed for mid and upper-level managers. However, others with comparable duties and responsibilities may attend. The course is available in part on a quota basis to industry personnel assigned responsibility under the industrial security management for effective application of classification, downgrade, declassification, marking requirements, as established by the Government.

In a broad sense, the scope of the course was to provide the student with a general knowledge of the history, policies, and implementation and management of the industrial security regulation in a fundamental working knowledge of all program elements. As a result of the determined efforts of the task force, a decision was made. First, that the proposed course could, in fact, be conducted, and, secondly, the responsibility to conduct the course was assigned to the Defense Industrial Security Institute there in Richmond, Virginia. However, it must not be overlooked that before the first course could be conducted, we at DISI had a formidable task to accomplish.

For instance, we did not have sufficient classroom space, nor instructional staff to accommodate this new course. Nonetheless, the wheels kept turning, and in January of 1974, the first two of our instructors for this course arrived. The third did not arrive until the middle of March.

A special note here should be made that in less than a year from the meeting of the task force to formulate DOI, the pilot, our first course of instruction, was actually presented.

This reflects the outstanding support and cooperation that we have received from all agencies concerned, and a lot of hard work on the part of the instructors.

At the present time, we still do not have sufficient dedicated classroom space. However, construction funds have been programmed and we should have better facilities within the foreseeable future. Until then, we will conduct our courses in the existing classroom wherever possible.

In those cases, where this is not possible, we have been assured that we can use the commander's conference room at the Defense General Supply Depot.

In view of the rather compressed time frame, the pilot course was conducted at the Defense Industrial Security Institute during the period 3 through 14 June 1974.

As previously indicated, the course was divided into two distinct segments, each one a week long.

Could I have the first slide, please?

The first week basically addressed the classification downgrading, declassification and marking, as you'll see in this slide and the following

slide. These sixteen topics were the bulk of the material, or the subject matter that was covered during that first week.

During the second week, these are some of the topics that also were addressed. In addition to the five representatives from industry who were invited to attend the pilot course, fifteen representatives from the Department of Defense agencies, the Department of State, the National Security Agency, and the National Aeronautics and Space Administration, also participated.

From the very valuable constructive criticism offered verbally during this course, we have greatly benefited, and I'd like to take this opportunity certainly for the five industry representatives and the Government representatives during that course, we certainly want to thank them for their assistance in this area.

During the course, we also requested written critiques or comments submitted by these attendees. There was general agreement that the course addresses all aspects of the information security program, and with some refinement and periodic revision, will prove to be a valuable tool in training new security managers and effectively stimulate the exchange of ideas between security managers.

This, you might say, concludes the first part as far as background and a slight overview, as far as the objectives of this new course. At this time, I'd like to turn the podium over to Mr. Fred Daigle, who will give us again that viewpoint of the industry regarding the course and his view of it.

INDUSTRY VIEW OF INFORMATION SECURITY MANAGEMENT COURSE
BY
FREDRICK J. DAIGLE

It was with a great deal of pride and appreciation that we, representing both industry, our own companies and the society, received invitations to attend the first week of the two-week pilot course, and this is another one of the examples of the society and DCAS working together as has been so ably described by Bob Green. I would be remiss if I didn't take a quick aside here to extend the appreciation of the entire society to Bob Green for the many, many kind things he said about us during his presentation.

Those invited from the society by the commandant of the school were Jim Buckland of Martin-

Marietta of Orlando, Florida, our NCMS Vice-President, myself, Jack Robinson, from the Center of Naval Analysis, editor of the NCMS Bulletin, and a member of the Board of Directors, Lyn Satterfield, Westinghouse, Baltimore, an immediate past-member of the Board of Directors, Gene Suto, General Research Corporation, McLean, Virginia, and now President-elect of NCMS. In addition to the above were the fifteen people from Government who Major O'Leary mentioned.

As an interesting sidelight: of the twenty course attendees, twelve were members of NCMS and two more joined during the week. You had to show your NCMS card to get a drink at the bar. One joined yesterday, Mr. Rae Nehls; and all the instructors indicated their interest and the intention to join with us in the society.

Prior to presenting a viewpoint relative to course content and its conduct, there is a prelude that must be discussed for the benefit of the NCMS membership. This is in regard to the advance publicity that we of the society have been hearing for well over a year as a result of presentations at our seminar, our mid year mini-seminars and at gatherings of other classification and security-related groups.

The general theme of this publicity was that the DISI school was going to conduct a course of instruction for classification management personnel in both industry and Government.

This particular course is not designed for that purpose as has been described so aptly by Bob and by John O'Leary.

Now, to the course itself. It was obvious that there had been much preparation for the course, and we cannot say enough of the dedication and the enthusiasm of the staff of DISI and the instructors.

The content of the instructional blocks was detailed and thorough even though it was subject to much analysis. Recommendations were made for elimination of some what we considered unnecessary material, a lower-key approach to certain facets of classification, updating of text, and a need to place greater emphasis on certain other factors.

These comments were all shared in the most part by the knowledgeable attendees.

At the outset, it became apparent that some of the attendees had no industrial exposure whatsoever in daily work requirements and as a result

could not understand the rather overwhelming comments and suggestions made by the industrial NCMS attendees. Thanks to Bob Green, who was also in attendance, and who very carefully restated the purpose of the pilot course indicating that industry and NCMS had been invited to insure that their views were made known, because among other reasons, Government security managers do at some time in their careers interface with industry in some manner, and to provide with industry in some manner, and to provide these managers with the ability to interface knowledgeably was one of the objectives of this course.

After the second day and after the foregoing opportunity to clarify the various participations, the critiques were most comprehensive and informative. There is little value in discussing the individual items of the critiques, as all attendees were informed by the school that these were well received and would be incorporated into the first regular session of the course, which is going on right now.

The Institute has assured me that the next year's schedule will be such that it will not conflict with our Washington seminar dates, thereby permitting the instructors, as well as the potential attendees, to attend the seminar if they wish.

The single critique item that was agreed upon by all attendees and worthy of reporting here was that although all the information was primarily factual, generally complete and well presented, it did not completely meet the primary purpose of the course, that being relating this wealth of data to the responsibilities of Government security managers in implementing the information security program.

This aspect was discussed in depth with the attendees, instructors, and the school administration, and there was no disagreement with the observation.

The second week of the course, that dealing with physical security, was to be restructured--over the weekend, I might say--with the Government security manager's responsibilities in mind, and I expect Mr. Larsen, who is your next speaker, will give the Government's viewpoint and will address this change in procedure.

In summary, we concur the material gathered for the course be modified as recommended and when reoriented, to the responsibilities of the Government security manager, will provide a very beneficial course of instruction for many an

upper-level management personnel, and is the first solid step taken to formally present any classification management training.

Hopefully, it will make our lives easier by giving our bosses a better insight into what we are trying to do.

However, we additionally recommend that the role of members of industry that are invited be specifically defined and stated in the invitation and in the opening remarks introducing each course.

Further, we submit the observation that we still feel a dire need for a course in classification management both for Government and Industry classification management trainees where they commingle and learn from each other.

We have long felt this need as being the first one that required fulfillment. When the classification management specialists have been taught, then a review of what they were taught would be most beneficial not only to Government security managers, but also the first and second level industrial security managers.

GOVERNMENT VIEW OF INFORMATION SECURITY MANAGEMENT COURSE

BY

MR. FRANK LARSEN (Navy-CNO)

This appearance is a two-fold privilege--not only to have the valuable platform time at this national seminar, but also to represent the twelve government departments and agencies which were represented at the two week "pilot" course on the DoD information security management program. In addition to the cogent remarks of Mr. Daigle about the course, it has been apparent the grapevine worked very well and most of you have received individual if not collective reaction first or second hand. It may be of interest for you to know, however, that a meeting was held in Mr. VanCook's office in OSD on 3 July 1974, at which time several of the pilot course participants from the Government essentially gave an overall critique. There was general agreement within this adhoc committee on several points which I'd like to relate to you now. I'm reminded at this point, of that great biblical guidance--"For God so loved the world, he didn't send a committee"--none-the-less, the interest, dedication and expressed desire to improve and promote this course on the part of DISI, DCAS and Mr. VanCook himself created a very evident singleness of purpose.

for this panel, and I blame it all on Dr. Kissinger, really, for since he has been promoted to Secretary of State, it has become rather fashionable, or the in-thing to do, to have someone with a foreign accent on a panel or on a committee.

Of course, he tried to get Dr. Kissinger, and when he failed in doing so, he went through the NCMS roster and found that I was the only one who filled the bill. It is remarkable, you know, that even in SAMSO today, I am suddenly being called "Doctor."

In any case, I'm very glad that George asked me to be here with you this afternoon.

Being with the Government and also being a relative newcomer to the NCMS, somehow I feel that there is a lack of comprehension on the part of some people as to the inner workings of the classification management office at the User Agency level.

Briefly, we at the working level have to implement and interpret the many directives and regulations emanating from higher headquarters. We have to rationalize, use good judgment, and, finally, develop and publish a meaningful classification guide.

To me, development of the guide begins the day the project officer or the program officer comes in and says, "We're going to let an RFQ, a request for bid in three months, or six months, or a year, and we'll need a classification guide as soon as possible.

At that time, the contracting officer, the program officer and the classification management office start to work. The development of a guide takes a considerable amount of time, and many times it never ends. It seems like when a contract has been completed in three or four years, we still get telephone calls on the interpretation of the classification.

Before I turn this meeting over to the panel, I would just like to say one word, that I believe that classification is born at the User Agency level. If you have any problems on classification, I would advise you first to come to the classification office that is indicated in your guide. If you have complaints, you may go to headquarters, but they come back to us anyway, and we will face the problem.

We are indeed fortunate this afternoon to have three representatives from Government who represent many years of experience and knowledge in many facets of security classification. The members of the panel will speak on their own background and from their own experience.

Mr. Murray Marker, who speaks on procurement activities and contracts; Colonel Griesmer will touch upon the role of a program manager in the research and development environment, while Mr. Joseph Care will address himself on the subject of preparing and issuing a classification guide.

Our first panelist this afternoon will be Mr. Marker. He received his law degree from Columbia University and after a number of years of private law practice, he joined the Federal Security Agency in 1939. There he was appointed to the Department of Commerce for International Trade, and since 1957, he has been Regional Counsel to the 11th Naval District in Long Beach.

I had the good fortune of listening to Murray before, and I believe that he is one of the foremost authorities on Government contracts and procurement.

PRESENTATION BY MR. MARKER

I expected to be the last speaker. I don't know what to say now.

Everybody else has said how delighted they are to be here, and I think I'd be keeping the truth from you if I didn't say that I feel the same way about it.

I had the opportunity as Gene told you to talk to the California group two years ago. I didn't know whether they enjoyed it, but I certainly had a hell of a good time, but I've been told they liked it, and I'm just going to tell you the same thing, too, they liked it very much.

I'm here under false pretenses, really. I am not truly the representative of what you call the User Agency.

The Naval Regional Procurement Office is the centralized purchasing for procurement office in Southern California, but by the time we get a request to contract for materials or services or for research and development operations, a large part of the work that comes from you, ladies and gentlemen, has already been done.

The technical people and the requirements people at the requiring activity have gotten together with security personnel. They've agreed upon or they have worked out what they think the security requirements are, the classification requirements are, and that's including the requisition which comes down to us, so that we get from you something that plays a part in what we do.

We don't participate in any of the decisions which are made on the security classification level. Captain Chapman told you about the armed services procurement regulations and how the committee works and told you that the armed services procurement regulations--what it is and how you do it sort of thing, and I think perhaps I might sort of fill out the picture by describing to you how we operate under the ASPR, and maybe when you get to the questioning period, if we get to the questioning period, you can try to place into perspective how what we do impacts on you, and vice versa.

I think the first thing to point out to you is that the basic concept of the operations that fall under the armed services procurement regulation is to follow the legal requirements for entering into a contractual arrangement with a contractor to either provide the services, the activities or to furnish the materials or the supplies of the activity.

There are two ways of doing this. The first, for the time being, anyway, and, traditionally, the classical way, is by advertising. Advertising--formal advertising--for bids does not fit the kind of operation that involves you, because if you have classification requirements with regard to any part of contract performance, there is an exception in the ASPR which permits you to negotiate a contract, rather than to advertise it, and so unless there is some rare exception, and I'm not too familiar with what they would be, there is very little--practically no connection--between those instances where the procurement is of a firm specification procurement for purchase of supplies or services without any classification requirement on it, so let me talk only about the second type of negotiation contract.

Without detailing the sections or the language or the specific requirements of the armed services procurement regulation, we start with the procurement request, the requisition that comes from the procurement activity, and this tells us what it is they want, how much of it they want, for what period they want it. The specifications will be either performance specifications which say, "We

want a black box that will do the following," or it will be a technical spec which will spell out specifically what the black box is to do.

What is the security classification required to provide the safeguards against some technical advance getting out and becoming known in areas through sources not too known that should not be permitted to know?

What are the areas in which the services will be performed, so that there might be access to classified documents or drawings, or information of one kind or another, or to classify security areas where performance by the Navy people, or the Air Force, or Army people, the same difference, should not be observed by people not properly cleared?

We receive this requisition, as I've indicated to you, and we analyze it from the point of view of what kind of sources we have to go to. Ordinarily, the requisition itself does indicate some sources, and we are required--assuming that there is no security classification--we are required to synopsize; that is, to publish in the Congress Business Daily, which is published by the Department of Commerce, a synopsis summary of what it is we are in the market for, so that interested companies can notify us of their interest and seek a copy of the solicitation when it is issued, so that they can compete.

If there is a security classification problem involved and this comes to us in the form of the attached DD 254, we do not synopsize. In most cases, there are some instances where a synopsis is issued for the purpose of finding out whether there are any companies in this field capable of undertaking the particular operation, but it would be an extremely general statement, one which would not be in any way indicative of what the security problem is or precisely what it is we want.

It could be a general description, for example, of certain electronic requirements, if you need an electronic finger, but without detailing what the requirements would be for performance.

Assuming no security classification problems, we do synopsize. Assuming the classification problem, we do not ordinarily synopsize, but we seek out those companies we know have a capability.

To companies which have been cleared, companies that ask for copies of the solicitation in order to compete, would have to satisfy the security

people of their clearance, and in that case I believe it's DCASR that does this for us.

Assuming then that we have a sufficient number of companies, or company--in many instances, we deal with the sole source--we have the companies that are being solicited. They've been properly cleared. The matter is taken care of within the rules of the security requirements that you've set up.

We solicit proposals from them, and if the proposals are to address themselves to the classified material, they, of course, must be classified.

I'll proceed now and cut it short. In every instance I mentioned something that has to be done. Bear in mind that if there is a security classification problem, that has to be done within the security requirements.

Technical proposals and cost proposals are submitted to the technical activity for evaluation as to technical adequacy and acceptability, and are analyzed and evaluated by our office as to cost.

You receive a technical evaluation from the activity indicating what companies have submitted proposals which appear to be satisfactory and acceptable and can do the job or are marginally acceptable, but can be made acceptable by some corrections or filling in of some omission, and all those companies which have submitted completely unacceptable proposals in the technical aspect.

This determines what we have come to know. This determines the competitive range, that is, those companies that are now within the range of possibility, probability of acquiring, achieving, being given an award, being successfully the winner of the contract competition.

Negotiations then follow with these companies to correct deficiencies, beef up whatever seems to be inadequately treated, to clarify those areas which are not too clear, which are ambiguous, and also to negotiate, to improve the price, the cost. We then request a final offer which gives the company an opportunity to now revise their proposal to include what had been agreed upon or negotiated because of the discussions, to improve their competitive position.

Now we have two different problems to consider. In those instances where what we need is an article or services which meet the requirements

at the minimum level--that is, they will satisfy even though they can be done better--we determine the winner on the basis of the lowest price among those who have come in with a proposal which meets our minimum acceptable requirement.

In most instances of the type of work we deal with, the research and development or developmental work which is on the borderline, perhaps, of research and development, where more than minimum acceptable position is sought, where we need the best skills, where we need what we can get in the sense of the most experience and the most likelihood of achieving some advance, some improvement in what we know exists or what we believe may be done.

The choice may be made on the basis of a scoring which will rank the best technical proposal at a higher level than others, even though the others may be at a lower cost, so that we may make a wall of higher cost arrangements in order to achieve the best technical results.

You can believe me when I tell you that that area is the one that is most productive of disputes, protests, and, generally speaking, the kind of hearthurn and headaches that we go through, but we do it.

It is legal. It is accepted and within the regulations. It's sustained, and, generally speaking, is approved by the GAO in cases where a protest has been made.

Once the award has been made and once the contract has been executed, of course, the security-problems again have to be taken care of. They are now contract administration problems, and, except in those instances where the PCO retains contract administration, they are the responsibility or they become the responsibility of the DCASR.

Even in those instances where we retain--so to speak--where the procuring contracting officer retains the administrative responsibility for contract, it is usually delegated to the technical activity so that if we let a contract or some developmental feature for one of the laboratories, that would require some specific skills or the background and experience of the particular individuals who have the cognizance of the technical requirements of this particular problem in the laboratory.

The laboratory will be the delegated administrative officer.

Then there's midway where the administration has transferred the DCASR with technical personnel made part of the team.

Now, that, generally speaking, is the process of procurement that we handle for the User activities. Now, I am not too familiar, frankly, with the preparatory work that you do before it gets into the purchase request, but a little more familiar with what happens after the contract is executed and becomes an administrative matter, because if there is a dispute, of course, then the administration comes back to us usually in a claim or contract appeal.

PRESENTATION BY COLONEL GRIESMER

I've always had the impression that security classification in the intelligence and operations fields was lot more straight forward and had fewer problems than in the research and development business. I have to say it's my impression because all of my experience for the past seventeen years has been as an R&D officer. I do know one thing for certain; they don't have Aviation Week working their side of the street. But seriously, I do believe R&D has problems not common to other areas. DoD Regulation 5200.1 has little more than general guidelines for the R&D manager who must develop a new security classification guide or whose program is undergoing rapid changes. It tells him he must develop a guide in accordance with established policies and procedures and that the guide should cover the transition through research, development, test, procurement and the other phases in the R&D cycle. It tells him to consider the issues of net national advantage, lead time advantage and cost before making classification decisions. But these are pretty abstract and they get even more abstract when you have some specific issue at hand and try to apply them.

Then too, the program manager generally has a more mundane set of problems. He is worried about the cost, schedules and performance of whatever it is he is trying to get built or buy. He probably looks at security problems in the same light as the "ilities," reliability, safety, etc. He knows they cost money, but add nothing in the way of technical performance. It is probably safe to say that the average program manager spends little if any time insuring that his program's security classification guide is complete, up-to-date and cost effective. I am sure it rarely gets the same kind of attention that his budget does and yet, unless his program is completely unclassified, the costs of security are in every line item of his budget. While classification requirements probably do not in most cases represent a large cost factor in individual programs, it is none-the-less significant when viewed in the light of classification

costs to the DoD as a whole. But it can be significant in individual programs too. I'll give you a couple of examples. I was involved in one situation in a satellite program office where a classified computer printout of satellite ephemeris data was being accumulated at an overseas tracking station at a rate of an inch per hour. Operations analysts planned to save these runs for diagnostic purposes for several months. It very rapidly became apparent that storage and destruction facilities would be overwhelmed unless drastic actions were taken. The station commander had pleaded for a shipment of safes from the states. The people who wanted the data were told to find a cost effective solution. They quickly came up with a few changes to the software program that eliminated the classified portions and retained the useful data. It turned out to be a solution someone should have thought of to begin with. This same program was a Special Access Required program--covered by the old Air Force Regulation 205-23--for long after it should have been. Resources at contractor facilities as well as government installations were needlessly consumed trying to follow the briefing, debriefing and record keeping rules long after the program had grown too big to be afforded any real protection under this system. While the program office recognized the situation and recommended changes to higher headquarters, approval was a long time coming.

Approval was finally obtained and contracts were subsequently renegotiated to reflect the change in security requirements. The total savings to the program as a result of this change was in excess of \$130K, with a \$105K reduction on one contract alone. And, I believe I can say--Gene Klein can verify this--that the change did not result in any reduction in the protection afforded to the sensitive aspects of the program that did require careful classification. As a matter of fact I know the change allowed concentration on the truly sensitive elements by deemphasizing the bookkeeping operations. AFR 205-23 finally got to the point that it was serving to focus attention on programs rather than offering them any "protection." Recognition of that was a long time in coming. I think the lesson to be learned is that security practices and classification need to be continually reviewed to insure that they are protecting what really needs to be protected in the most cost effective manner. Regulations ought to be changed or eliminated when they don't do the job intended.

Which brings me to my next point and that is the need for program managers to find some method, a

method that suits their own program's needs, to insure regular review and updating of their program's security classification guide. The Air Force tries to make users aware of the need for this on a continuing basis with a paragraph in all guides which solicits constructive comments from users in the event classification imposes requirements for protection that prove impractical, progress of a program necessitates classification changes, or some other problem arises. From experience I've found that few users took the time to respond to that invitation. We would hear from a user in the event classification requirements suddenly generated a major problem. However, in general, the less pressing and far more common instances of not very clear language on certain entries in a guide, over or under classification, for example, were rarely brought up unless the program office took some specific action beyond the standard request printed in the guide itself.

A technique which we used in the satellite program office I referred to earlier and which did surface needed changes, was to hold regular, two to three times a year, meetings to hammer out changes--and I use that verb advisably. Program office personnel chaired these meetings that were attended by contractors, the Commands using and supporting the system as well as classification management specialists. With every interested agency involved in developing acceptable language, I think we ended up with a better--but more important--a more useful product. I don't think this was a dilution of the government's responsibility to properly classify national security information; on the contrary, I think everyone left with a better idea of why certain information had to be classified and equally important, the right words in the guide to assist proper application of classification guidelines. These sessions took time, but they were productive. I found the contractor people particularly cost conscious; they pointed out many areas of over or unnecessary classification. This was quite a dynamic program where I think this technique was necessary to quickly surface and effect necessary changes; other programs may not need this sort of concentrated activity, but every program should have a formal and regular mechanism for reviewing and updating guides. Letters to users for example, could take the place of meetings. On my present program, the Advanced ICBM Technology or MX program, we have begun a review of the present classification guide to eliminate over classification. I don't believe in the general ground rule that since this piece of equipment or data might someday be part of an operational system that it must

necessarily be classified for that reason. There is a tendency to always be on the safe side, but that does cost money and after a little probing I have generally found rationale for classification lacking.

The classification management staff at our SAMSO Headquarters spurs the program managers with an annual review of all guides. They push the program offices to insure uniformity and of course their across-the-board coverage of all programs does contribute significantly to keep the quality of our guides high. I have found all of these useful in keeping guides for which I was responsible as current as possible.

One problem that I've frequently encountered with classification guides involves specific vs general entries. On one hand the guide may cover many specifics in great detail; in the opposite situation the references in the guide are so vague as to be of little assistance in proper classification. There is a danger with the too specific approach too; if the user doesn't find the specific detail he is looking for he naturally assumes it is unclassified since the guide goes into great detail on many other points. In both of these situations the user isn't helped very much by the guide. I don't really have a good answer for this situation. From my experience I think we tried to make our guide as specific as possible, but still leaving some room for interpretation to encourage users to use their heads. Even with all the guidelines, classification is still mostly common sense and we need to keep reminding users of that fact. There just isn't anyway to cover every conceivable question; common sense in many instances has to be the ultimate arbiter.

One aspect of updating guides that has always bothered me is how to get the new information to all the holders of the guide. For guides classified SECRET this is probably not too challenging as they are individually controlled. But SECRET guides are probably a minority. For uncontrolled guides and especially where local reproduction of guides is authorized, I have never been certain that updates get to all the agencies having guides or to all the individual copies within each agency.

I have tried to enumerate a few of the problems I've encountered as a program manager in the area of security classification and how I dealt with them, hoping that my experiences might be beneficial to others. I do want to return briefly to a point I tried to make in the

beginning and that is that the R&D manager himself must in most cases decide what needs to be classified, at what level and for how long. Higher headquarters may approve guides but it is really the R&D organization itself, with able assistance from the classification management specialists, that decides on the gut classification issues. This is often difficult with only abstract guidelines to follow, but it is the organization that knows the data best and in the long run the organization that has to do the job.

PRESENTATION BY MR. CARE

It is truly an honor to be invited to sit with this panel and to discuss with you some of the User Agency functions and problems. My comments will be brief in order to allow ample time for questions.

Before we get into User Agency functions let me give you a brief rundown on the Naval Underwater Systems Center. We are a DoD shore activity under the Command of the Chief of Naval Material. Center Headquarters is located in Newport, R.I. under the Command of Captain M. C. McFarland. The Center operates facilities in Newport, Rhode Island; New London, Connecticut; Andros Island, Bahamas; The Azores; Tudor Hill, Bermuda; Fishers Island, New York; Seneca Lake, New York; Dodge Pond, Niantic, Connecticut; Millstone Quarry, Waterford, Connecticut; and Field Stations in Fort Lauderdale, Florida and one here on Harbor Drive in San Diego. Some of the skills we utilize at the Center are physics, acoustics and hydrodynamics; electromagnetics; applied mathematics; metallurgy and materials research; organic, inorganic, and physical chemistry; electronic signal processing; servo mechanics; miniaturization and instrumentation; mechanical, chemical and electronic engineering of considerable depth; operations research; computer science and oceanography.

The Center is currently involved in some several hundred projects, eighty percent of which are classified. A sizeable portion of our research is contracted to industry. That is what I am here to talk about, our role as a User Agency. Problems associated with NUSC as a User Agency begin at the beginning.

Let's take a look at a case in point. A NUSC project engineer has been talking to a competent well known independent engineer about a certain problem. He determines that this engineer has the expertise to help solve this certain problem. He also knows that the independent engineer was previously associated with a cleared industrial

firm that did considerable research in the current problem area. The NUSC project engineer then discusses a contract arrangement with the independent engineer. Suddenly he realizes that he must look into the security status of his prospective contractor. The two engineers arrive at the Security Office, both sure of one thing: Our prospective contractor needs a clearance for access and somebody will wave a magic wand and PRESTO! Secret Clearance. After the storm, we settle down to a standard request to the cognizant DCASR for a Facility Clearance for this on-the-spot, newly formed Research Corporation. The request indicates the level of clearance and stowage capability required, the address of the Corporation, and most important of all it reflects an urgency for an interim clearance so that we may commence contractual activity almost immediately! Does that sound like a full afternoon? It is! And we, believe it or not, respond and provide the service as expeditiously as we can. Is it poor planning? Not necessarily. Our engineers get a task assignment and they start digging for the best way to provide the fleet with the tools and knowledge they need as soon as possible, and that "as soon as possible" might very well be the only lead time we have in this particular area over a potential adversary. It is TIME that we are buying, and it is TIME that classification buys us, nothing else.

Most of our classification actions are derivative rather than original. Therefore, the guidance we provide a contractor for the most part is based on guidance we receive with each task assignment from such DoD Components as NAVSHIPS and NAVORD that have now combined operations and are identified as NAVSEA; NAVLEX; ARPA; CNO; et cetera. From this basic guidance we develop DD 254's for those portions of NUSC's task assignments that are let out for contract. If the scope of the contractor portion warrants it, we include the original guidance as an enclosure to the DD 254. Some problems crop up along the way. There are occasions when neither the cognizant engineer, nor the Classification Manager can agree on the appropriate level of classification or the proper downgrading designation that should be applied to a contract task. Interpretation of the original guidance is generally the problem area and that is soon resolved by contacting the originator of the guidance. Another problem here is that, unfortunately, there are still those among us that interpret guides to their extremes and classify forever. I use that term "forever" because I feel that in some areas 30 years is "forever." Some valuable assistance came into being recently via OPNAVINST 5510.132 dated April 10, 1974 entitled "Preparation of Security Classification Guidance." What is most encouraging is outlined in paragraph 3 under "Classification

Philosophy" and I quote: "Classification decisions should not be made based on "gutty" or "spur of the moment feelings." Somebody, God Bless him, finally hit the nail on the head. Paragraph 3 continues and goes into what I consider an intelligent approach to the preparation of classification guidance. One of our other major problems as a User Agency is the release of documents to industry. WHO CAN HAVE WHAT and for HOW LONG and WHY CAN'T HE HAVE IT are the subjects of a great deal of correspondence. The easiest way to respond to a request for documentation is to deny the request. Somewhere one can find a reason for denial, but we all know this isn't the answer. Release of contract related documents to industry is very necessary and the temporary or permanent custody of any such documents by industry is not expected to result in the total downfall of the National Security. Here at NUSC all requests for documentation are routed via our newly formed Distribution Center for processing. The procedure that has been established insures that the prospective recipient of classified material has a facility clearance with proper stowage capability and a need certification. Each outgoing document is also checked for possible downgrading or declassification and other necessary security markings prior to its departure. Unclassified material is checked for distribution limitations, if any, with emphasis on releasing with Distribution Statement "A" whenever possible.

The protection of classified material is still our biggest worry. The TIME element places a great deal of pressure on both Contractor and User Agency personnel. This in turn encourages shortcuts or by-pass of security systems by both parties. As I stated previously, TIME is what it's all about and to compromise an entire project by shortchanging security requirements defeats the whole purpose.

In conclusion, I would like to parrot some remarks by Past President Jim Bagley that he made at the 1972 seminar that are, in my opinion, an answer to many of our problems:

The most urgent priorities should be:

- (1) The establishment of job standards for classification management personnel.
- (2) The development of education and training programs at all levels.
- (3) The recruitment of new people, hopefully younger, into classification management.

- (4) Steps to establish courses at the college and university levels.
- (5) Bring into the field of Classification Management, information and technical information specialists who are also concerned with information which may be released and information which must, for a time, be protected.

QUESTIONS AND ANSWERS

MR. TITKO: I'm Mr. Titko. I have a question for Colonel Criesmer.

Colonel, at what phase of the development process do you put a security classification guide into practice?

Ideally, I suppose it would be when 254's are being generated, but that in many cases is not feasible. Now, operational phases, operational tests, development tests, pre-ITR or ITR.

COLONEL GRIESMER: Well, I've had experience with guides that were written for exploratory development programs, for example, and I'm sure there are some that probably ought to be written before they even get to that state.

I really don't think there's a universal answer. I think it depends on the particular area that's involved. But we have 6.3 programs and 6.2 programs within the Department of Defense, both of which were security classification guides, so I think it depends very much on the type of information you're trying to protect.

In many cases, a guide may be required to go through the whole lifetime of the system. The system may spend many, many years in the early R&D stage before it goes into production and a guide may be necessary in the early years. The guide will change as different things are important in different periods of time. In summary, each program must determine the what and when based on its individual needs.

MR. KLEIN: I have a question for Murray. I'd like to know how you go back and estimate the security costs on your program in setting up a contract? How is that done?

MR. MARKER: That would be the function of the proposal and its evaluation by both the technical people, the classification people, as to the rates involved, the overhead, and so forth. It would be a key method, but not necessarily combined. It might be a sequential operation.

MR. KLEIN: Is that negotiable?

MR. MARKER: The cost may be negotiated in the sense that perhaps the provision for the meeting of the security requirement may be overemphasized. It is not in the main negotiable. It's a firm requirement that has to be met.

MR. CHELIUS: Colonel Griesmer, you now have offices like in your MK Program. You have offices also at the headquarters level and the AFC levels. Do you find that the guides are widely distributed within the program offices at higher levels?

COLONEL GRIESMER: I'm probably more familiar with the guides on the program I was on before. I know they were, and they were distributed to Air Force Headquarters as well as OSD.

I'm pretty sure that program officers or the monitors up in headquarters have guides for their programs, but beyond that within the headquarters, I doubt it very much.

That's probably a good point.

MR. DAVIS: Henry Davis, LTV Aerospace. I'd like the panel to address the question of what the contractor should do when he gets the DD 254 written in 1974 that is still spelling out the old Executive Order?

MR. CARE: Send it back.

I'll tell you, you'll soon find out what to do when DCAS makes an inspection.

MR. DAVIS: They did, and did nothing.

MR. CARE: Well, I'm sorry to hear that, but we've had this problem and they get away from it once in a while. We don't profess to be perfect, but I'd send it all the way back.

MR. BOWERS: My name is Bowers, from Westinghouse, Annapolis, Maryland.

Basically, my question is to Mr. Care about the point for reviewing for retention. What criteria do you use for determining authorization to retain and just what steps do your people go through to make this determination?

MR. CARE: Sir, we don't usually deny continued retention after the Contract expires. The Manual allows a retention period of three years after expiration of the Contract. Even at the end of the three year period, if a continued need to

know exists we allow further retention for a specific period. We look into WHY you need it. Generally we find that the Contractor is doing work in another related field. Based on this, a need to know can be justified for a certain period of time. Unfortunately, we cannot authorize retention forever.

PANEL: PROTECTION OF COMPANY PROPRIETARY INFORMATION

MR. W. PETE DENNISON, Moderator
Head, Security & Safety
Hughes Aircraft, Torrance, California

MR. RICHARD J. HEALY, Panelist
Head, Security and Safety Department
Aerospace Corporation, Los Angeles

MR. RICHARD A. BARDIN, Panelist
Attorney, Fulwider, Patton, Rieber, Lee & Utecht
Los Angeles, California

MR. LORIMER F. MC CONNELL, Panelist
Assistant Secretary
System Development Corporation
Santa Monica, California

PRESENTATION BY MR. DENNISON

Good morning. Our panel this morning is Protecting your Proprietary Information, and as all of you have, I have been involved in security for many years, but my exposure has been with general security, not any specific area, however, due to many instances too numerous to relate here, I've found myself more and more involved in the subject of this panel.

Even though I consider myself a neophyte, I was very pleased when I was invited to moderate this panel, and before I introduce our first speaker, I would like to say that we are starting late and we had very little time in the first place, and each one of our panelists has been allotted a certain amount of time, so at the end of all the presentations, we will take questions and try to answer them.

PRESENTATION BY MR. HEALY

The information I'm going to discuss is taken from a book, "Protecting Your Business Against Espionage" published by the American Management Association, written by Timothy J. Walsh and me. If any of you are interested in obtaining the book it is generally available in your public library.

Industrial espionage and the protection of information isn't new. It goes back to the silk secret that the Chinese developed about five thousand years ago. As you may know, the Chinese were responsible for actually developing silk and they kept the process a royal secret for a matter of three thousand years. They kept it within the royal family because it was so important to the country. Actually an inside job was responsible for the loss.

It happened that one of the rulers of the country nearby asked the Emperor of China if he could have some material to make silk. He was, of course, refused, but he tried another tactic. The Emperor had a daughter, and he asked the Emperor if he could marry his daughter. The Emperor agreed.

The outside ruler then sent an emissary to talk to the daughter and suggested to her that they didn't have silk in his country. She was told she would have to wear goat hair and other rough material when she arrived unless she brought material to make silk with her. So, she concealed silk worms and mulberry plantings in her headdress when she left the country. She later cultivated the silk worms in her new homeland and this is the way the silk secret got out of China.

This was just before the birth of Christ, so they were able to keep the secret a matter of three thousand years before it got out of the country.

They were rather severe about protecting the secret. If anybody revealed the secret, it was death by torture. They even developed a cover story that they released throughout the world in those days. They released information that they had developed a process of making silk by putting wool out in the sunshine and then after sprinkling water on it and combing it, it became silk.

You can imagine the research and development that must have gone in an effort to capture the secret. This is just to indicate that the protection of secrets is not a new problem, but one that has existed for years. We have it especially in the world today because of research and development.

We are told that in 1920, the research development of this country was worth only ninety million dollars. This had increased to twenty-six billion by 1969, and the next slide will show that it had increased to twenty-nine billion

in 1972. Further, that in 1973 it was \$31 billion. So, it seems obvious that research and development in the country is a very valuable commodity and one we must safeguard.

We some times do not realize how many new products have come onto the market in the last 25 years. Many products have changed our way of life such as TV.

Let us first take a look and see what might be considered target information or that which other people would like to have.

First there is research and development information. The second is production data, marketing information is third, and finally, general business data. We will examine each of these areas in the time left to us.

The first--research and development--can be found in every organization, regardless of the kind of business. A janitor cleaning company or a guard company, for example. Each has research information developed to help make a better product or to sell their products better. It has been said that any organization that does not have information to protect is not competitive. Therefore, research and development information in every organization is important.

An example of the theft of research is what I like to refer to as the great Arles caper. Dr. Arles was a teacher at the Brooklyn Polytechnic Institute. He was quite a brilliant man. He did consulting work for the Government and many other organizations; he held some fifty patents; he had three degrees, a law degree; a degree in chemistry; and a business degree. You can see he was well equipped educationally. He was also in "Who's Who" and had a worldwide reputation.

He was teaching night classes at Brooklyn Polytechnic Institute and he had a number of engineers and scientists in his class. He would say to these people in his class, "Now, I don't want just ordinary information that you deal with on a daily basis when you write your papers. I want you to tell me about interesting things. If you give me the right information, you can be sure of a good grade." As a result, he began to collect information from these students, and in this way obtained very valuable information.

In this way he obtained information from three companies--Sprague Electric, Merck and Robm and Baas. Merck first found out about this problem when they heard that Arles had given a lecture

in Toronto, Canada, and talked about a brand-new formula that he had developed to neutralize a chicken disease that had been wiping out chicken flocks all over the world for many years. Merck regarded this as about a twenty-million dollar business a year. Also, Merck had spent about a hundred million dollars on this research over a period of many years.

The Merck officials couldn't figure out how Arles had arrived at this formula developed by their company. At about that time they bought a French company, and in the assets of this French company was this same formula. The Merck people naturally asked "Where did you get this?" The reply--"We bought it from Arles."

Merck began an investigation immediately and when they looked at this formula, they found the formula was a copy of a Merck Company document. It hadn't been changed. They concluded that Arles had access to Merck research and development information. Finally it was determined that an engineer who was not even in the group that developed the formula had gotten into the laboratory where this formula was being developed. He had stolen the formula as well as cultures and sold all the material to Arles. Arles had also promised him a royalty for the worldwide distribution of the formula and so he could have obtained a great deal of money from his arrangement.

Merck then immediately started criminal proceedings against Arles and also filed a civil suit. However, Arles skipped the country and is reported to be living on the Riviera on the southern coast of France. He is a millionaire because of all the money he's gotten from his activities.

Merck Company was awarded a six million six hundred and thirty-eight thousand dollar judgment against Arles. Merck officials report they have the judgment framed in the Board room and it's worth exactly the amount of the paper it's written on. They have never been able to collect a dime from Arles.

Arles also obtained a formula from Sprague Electric, and Sprague got an eight million six hundred thousand dollar judgment against him. Rohm and Haas got a six million dollar judgment because of data they lost to Arles. These three companies obtained judgments of more than twenty million against Arles but none of them have been able to collect anything.

Last year there was an article in "Newsweek" stating Arles is now filing company names in

foreign countries. One of the names was "Exxon" in various countries throughout the world. Exxon spent millions in developing this new trademark. They may now have to pay Arles to use that name in a number of countries.

Let us next consider production information. There are certain production techniques that are very valuable. For example, Coca-Cola has one ingredient in their production that's called "X." From time to time a couple of the top people in the company mix up the basic material.

Next is marketing information. A striking case of theft of market information involved a man named Mayfield. Mayfield was a young trainee with Procter and Gamble in Cincinnati. Mayfield elected to leave Procter and Gamble and go to another company but before he left, he obtained the marketing plan for the next year for Crest toothpaste. Procter and Gamble valued the plan at about twenty million dollars.

Mayfield then called an acquaintance of his with Colgate-Palmolive in New York and offered to sell the marketing plan for twenty thousand dollars. The man from Colgate reported this to his top people and they in turn reported it to the FBI. The FBI indicated they should go ahead and make the arrangement. Twenty million dollars worth of information for twenty thousand dollars--a very good bargain.

Mayfield arranged to meet his contact from Colgate in the men's restroom at Kennedy Airport in New York. He also developed the code names, Mr. Crest and Mr. Colgate, because I guess he thought you have to do that in this kind of business. When they arrived, they identified themselves as Mr. Crest and Mr. Colgate. Mayfield then directed his contact to go into one booth while he went into an adjoining booth. He then told his contact to pass him the twenty thousand dollars and his pants under the booth. In return he handed the plan to the contact. As soon as he got the plan, Mayfield ran out with the money and the pants into the waiting arms of the FBI. He was characterized by the judge in the criminal proceedings that followed as just a foolish young man. He got probation and then disappeared from the scene. Spies are not that stupid, ordinarily. There are some very clever fellows.

The next area is business information. This can be described by four P's--Plans, Performance, Prices and Problems. If you know any one of

these things about what your competitor's doing, you could be pretty safe in competing with him and giving him a lot of trouble.

Next are the threats that we have to deal with. There are really two. There's the external threat and the internal threat. First, the external threat.

The external threat is personified by the industrial spy. The individual who is really intent on getting information.

The industrial spy may use an undercover operator. The spy will probably not come into a company himself to get the information, but he'll probably hire somebody to get information. He will put the undercover operator in the company in the area where he wants to get information. Then he will collect the information he wants over a period of time.

These fellows are clever. They will not ask the undercover operator right away for the information they want. They will ask him for useless information. Sandwiched in between the useless information will be the real information the spy wants. The idea here is that the undercover man never knows what he has stolen if he is caught.

Another method is to use a patsy. The spy will locate a disgruntled employee or a financially troubled employee. He will then approach him to determine if he can obtain information from him. As with the undercover employee, he asks him for useless information but mixed with the useless information will be the information he really wants. If the patsy is ever discovered, he does not know what he has given to the spy.

Another technique utilized by the spy is trespass. He may also pose as a customer or visitor.

Listening is another technique. The olive and the martini has gotten a large amount of publicity over the years. However, the effective spies will tell you that the last thing they want to do is practice eavesdropping and wire-tapping. It's too difficult to do. There are just too many other ways, as you can see to obtain information.

Trash and scrap is another method. Intelligence people the world over utilize the technique of sorting trash and scrap to obtain valuable information that has been discarded. There's one story about an industrial spy that attempted to bribe a janitor so he could obtain the trash and scrap of a particular organization. He found

out that another spy had already made arrangements for the waste material. So, we should remember that material in handwritten form which has been discarded is just as valuable as the material that finally comes out in a perfect copy.

Another technique is the use of the applicant interview and resume. This is a very easy way to get information. The spy may also make up a survey and send it around to target people. These would be people he knows have the information he wants. He may ask for a large amount of useless information but included with the useless information will be a request for the area of value to him.

With regard to the applicant interview, the industrial spy will put an ad in a paper and advertise a position involving a particular skill. Hopefully he'll get an applicant from a particular company that he wants. He can then interview the applicant at great length. If he doesn't have the capability of conducting a technical interview, he may bring somebody that can. Of course, an applicant is always willing to make the best possible impression and will be anxious to supply information to prove his qualifications. The spy may also ask him to write the information down in detail.

The applicant is interested in impressing the interviewer, of course, because the job is always made most attractive.

Another technique of obtaining information is through a merger offer. Again, there have been some unethical companies in the past who have offered to merge with a company in which they wanted information. As a part of the merger negotiation access to the books of a company will be obtained. After the information wanted has been obtained, negotiations will terminate. The "Wall Street Journal" reported last year that not many companies will not deal directly with another offering a merger. Instead, negotiation will be done through an attorney or some neutral party.

Reverse engineering is another technique. This is legal. It was been reported that the first General Motors car off the line in Detroit is bought by Ford and sent apart to see what they've done that is different and new. This is also done by the other manufacturers. Then an effort is made to engineer around patents.

Subcontractors should not be overlooked. They may be inside as well as on the outside. If a

reproduction facility is being used, it should be remembered that valuable material may be sent out to be reproduced. There was a case reported last year which involved data belonging to the Monsanto Chemical company. A sensitive Monsanto report from a reproduction facility was obtained by a meat salesman who went to a competitor and offered the report for five thousand dollars.

It turned out that Monsanto valued the information at half a million dollars. The thief couldn't believe it when he learned the value of the data. It was reported that the meat salesman had a friend working in the reproduction facility who gave him the report. He was a salesman, so he tried to sell the report.

Then there is observation. This can be done in any number of ways. A rather striking incident, involved a case in Texas. DuPont was building a new plant there and the configuration of the plant had a great deal to do with the manufacturing process. A competitor hired a photographer to fly over the plant site from time to time and take pictures. Apparently, he flew too low and the DuPont people got suspicious. They got court injunction when they found out pictures were being taken.

The various aspects of external threat have been covered.

Next, we might consider the internal threat. The internal threat is personified by employees generally. The disloyal employee is certainly a threat. He may, for one reason or another feel that he's being mistreated by the company.

One particular case involved a chemist by the name of Fox at American Cyanamid. Fox became disgruntled because he thought that he had not been promoted adequately and that his salary increase was inadequate. So he decided to steal from the company.

He formed his own company. He eventually was able to obtain enough data so that he was able to quit. Later he sold his company to an Italian company. His activities were uncovered because he talked some of the people working in Cyanamid who were caught.

The mobile employee is also a potential threat. In these days, particularly in the scientific areas, an individual can go across the street and get a twenty-five dollar a week raise without any problem at all. We have a mobile society, so we must be careful of the people that are moving from company to company. They may be doing this purposely to collect information that can later be sold.

Also, there is the moonlighting employee. These days many individuals are required to moonlight to make ends meet.

Marketing employees are also vulnerable. Marketing people are naturally aggressive, outgoing, and they want to make a good impression on potential customers. How much and the kind of information they give out may be important.

Another area is purchasing. The employee in purchasing may be buying material for the company. He wants to get the best buy for the company as well as the correct material so he should be instructed to be careful that he does not give too much information to the vendor. The vendor may then go down the street and give the information to a competitor.

There are a number of miscellaneous employees. This includes the employee that runs the projector in the Board room, the secretary who knows as much about her boss's business as he does, and the janitor, who may be working in sensitive areas when no one is around.

Consultants are ethical, in general, but they should be considered a potential problem and be included in the information protection program.

The publications area can also be troublesome. Seminars and trade shows should be considered. Control of material going into publications such as sales brochures, etc., is essential.

When an individual attends a seminar he will try to make good impressions for his company. He may want to talk about his work to other attendees.

In summary, then, we have outlined the various types of information that may be vulnerable to loss. We next discussed how sensitive data may be lost--through the two types of threats, internal and external. The next phase of a presentation such as this would be to outline safeguards that should be adopted to protect data. However, we do not have time for such a discussion.

PRESENTATION BY MR. BARDIN

TRADE SECRETS

I. Nature and Definition

A. Widely Accepted Definition--

"A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it.

B. Typical Categories of Trade Secrets

1. Formulas
2. Methods of Manufacture
3. Processing Techniques
4. Prototype or Sample Items (not yet publicly released)
5. Compilations of Technical Information (e.g., drawings reflecting dimensions and tolerances and other results of engineering effort)
6. Source of Supply
7. Business Plans (e.g., introduction date of new product)
8. Sales Information (e.g., lists of customers, contract information and the like)
9. Key Employee Information (e.g., salaries and benefits)
10. Computer Programs
11. Scripts of Plays and Motion Pictures

II. Legal Basis of Trade Secret Rights

A. Protection Against Breach of Trust or Faith

B. Confidentiality Obligation May Be Based on Express, Oral or Written Contract (e.g., employment agreement), Implied (e.g., under employment relationship), or by State Statute (e.g., Calif. Labor Code)

C. Improper Means of Discovery

D. Criminal Statutes

III. Patent and Trade Secret Rights Distinguished

A. The protection accorded to a trade secret holder is against disclosure or unauthorized use of the secret by those to whom the secret has been confided under express or implied restriction of non-disclosure or non-use. It also protects against disclosure or use when knowledge of the secret is gained by some "improper" means (e.g., wire tapping). No protection is afforded against discovery by fair and honest means (e.g., from sales literature or other technical literature, independent creation, accidental disclosure or reverse engineering. Novelty in a patent sense is not required, but a trade secret, according to the prevailing view, must exhibit some minimal degree of novelty.

B. Patents are granted under the Federal Patent Act which has its basis in the Constitution. Patentable subject matter is limited to a "process, machine, manufacture, or composition of matter, or ... improvement thereof." Novelty, utility and non-obviousness are required. A

limited right to exclude others for the statutory period of 17 years is granted once the patent issues. Independent creation is no defense.

III. Loss of Rights

A. Subject Matter Becomes a Matter of Public Knowledge or of a General Knowledge in the Trade or Business

1. Disclosure in a Patent or Other Publication
2. Disclosure Inherent in the Item Sold (subject to reverse engineering)
3. Disclosure at Trade Shows

B. Disclosure of a Trade Secret to Another in Confidence or Under an Implied Obligation Not to Use or Disclose Does Not Divest Rights

1. Disclosure to Employees Having a Need to Know
2. Disclosure to Licensee
3. Disclosure by Customer to a Vendor
4. Disclosure to Potential Investor

IV. Practical Effect of Trade Secret Rights

A. Protects Against Discovery by Unfair or Unlawful Means

1. Breaking and Entering
2. Compromising Employees
3. Aerial Surveillance
4. Industrial Espionage

B. Protection Against Misuse by Those Who Have Lawfully Acquired Knowledge (Most Common Problem Area)

1. Employee or Agent
2. Consultant
3. Licensee

V. Litigation

A. Legal Theories

1. Breach of Contract
2. Breach of Trust
3. Interference with Advantageous Business Relationships
4. Unfair Competition
5. Conspiracy
6. Anti-Trust
7. Improper Means of Discovery

B. Course of Suit

1. Complaint

2. Restraining Order and Preliminary Injunction
3. Discovery
4. Trial
5. Judgment

- a) Damages
- b) Injunction (perpetual, or limited, based on headstart theory)

6. Contempt Proceedings

C. Settlement

1. High Percentage of Controversies Settled

D. Inherent Problems

1. Plaintiff Must Carry the Burden of Proof (difficult to show that subject matter is, in fact, secret)
2. Risk of Further Disclosure of Secrets of Both Plaintiff and Defendant

- a) Protective Order

VI. Factors Tending to Influence Courts

A. Taking of Documents and Other Physical Items

B. Effort Made by Plaintiff to Protect Information (e.g., use of employment agreements, visitor control, limited access at plant areas, briefing of employees on confidentiality)

C. Time Interval between Former Employment and Introduction of New Product or Start-Up of New Business.

D. Efforts of Defendant to Compete Fairly

E. Strong Public Policy Favoring the Right of Individual to Practice his Chosen Profession

VII. Areas of Common Misconception

A. No Written Employment Agreement is Required in Order for an Employee to be Under a Confidentiality Obligation

B. Trade Secret Protection Extends to Both Information that Is in Writing and that Which Is Not in Writing

C. Provisions in Agreements Restraining Former Employees from Working for a Competitor are Void in California and Many Other States, Except Under Special Circumstances (e.g., in connection with the sale of a business)

D. Inventions Conceived During Period of Employment but Later Reduced to Practice Likely Belong to Former Employer.

PRESENTATION BY MR. MC CONNELL

When I was asked to make a presentation, I wasn't quite sure what I could contribute in addition to these two very prominent gentlemen who preceded me. They've given you just about everything that you could possibly want to learn on the subject. But I thought it might be of interest to you to know specifically what one company does in the way of trying to protect corporate information, so that you might compare this information with how you organize to protect your proprietary information. Figure 1 gives you an idea of how the functions are clustered at System Development Corporation. Our company's business is information technology; for example, we furnish services in the development and manipulation of large data systems, and in training people to use such systems; we also operate such systems. So, information is a very important commodity to us, and over the years we've found it makes a lot of sense in terms of our internal business operations to gather all of the corporate information control functions under one manager. Not only military security classifications, but functions of proprietary information control are found there. Also, the corporate policy, procedure and forms functions work nicely for us combined in the same organization.

We have a system for document review which pertains to all aspects of information control. Figure 2 illustrates a universal form which enables us to put a document through any kind of information review process desired--be it for export, copyright, military classification, or trade secret control. There is a section at the top of the form that indicates various actions that one might want to request--from initial "publication" to "dissemination," to "classification" or "other" review. We have a section midway down on the form for "classification," and there are two types: "military" and "corporate." Documents being reviewed for whatever purpose--initial publication or outside release are looked at from the standpoint of the proprietary value to the company as well as possible military classification. For example, if it's a document that someone wishes to release to the public, we consider whether it should be copyrighted or not. So, we attempt to take all possible information controls into consideration at the same time in a single review process.

Figure 3 shows a page out of one of our policies and procedures which outlines the various SDC document review processes required. I simply want to make the point here that we consider it important to have published procedures that tell people precisely what reviews are required within the company.

I think Dick Bardin mentioned that if you're going to try to protect trade secrets, it's important that you have some kind of system that makes it reasonable to believe that you will really protect your trade secrets. In this regard, we think that it's important to have a good corporate documentation system which people understand. We define a documentation system as is indicated in Figure 4. Some of our documents are intended strictly for internal consumption; we have a particular series of documents called Notes and we encourage people to write all preliminary, rough, working technical information in this series--with the understanding that their Notes will not be disseminated outside of the company. This encourages the entry of many "uncut diamonds" into a system where protection is possible.

We have another series of documents which we call TMs, written with the understanding that they might well and probably will be distributed outside. TMs receive greater editorial attention and more extensive review.

Now, I didn't realize this when we established our documentation system, but Dick Bardin pointed out to me later that our document series serves our patent function also, in that it serves a function similar to the engineering notebook. If you have a corporate series of documents with reliable functions for central recording and archives, then that kind of does what your engineering notebook does. I was very pleased to learn that because, as you know, it is often difficult to get engineers to write everything in their engineering notebooks. Some people who have been with us for years and terminate turn in blank notebooks. But they have written Notes, so we do retain technical information in that manner.

An outline of the elements of our proprietary information control program are shown in Figure 5--the front page of our Policy and Procedure Directive on Protection of Corporate Information.

As I've said, at SDC we're very much concerned with the protection of proprietary information. We've examined possible ways to protect computer programs, for example. We've looked at the possible opportunities of patent or copyright

protection for computer programs and we've pretty much concluded that these aren't very effective. These may not even be available protections under the law. Also, patent protection doesn't seem to be a good idea for computer programs. I'm sure you've all seen telescoping shopping carts in the markets; someone who got the idea to do that has the patent on it; the invention is out there for everyone to see and it would be quite obvious to the inventor or the owner if anyone started infringing. But with a computer program, it's a different thing. You can't see it or touch it. It's invisible electronic bits of information. If someone steals your computer program, puts it on his computer and uses it, it isn't at all obvious to the general public that it exists. In other words, it is very hard to detect the theft and the unauthorized use.

We have therefore concluded that it is best to rely on the trade secret method of protection for most of our things. We do patent a few items and we employ copyright protection for our published documents; but trade secret is our most important means of protection.

Another area that I don't think we've touched on yet, but which I think deserves attention is the area of protection of information required to prevent intrusions of privacy. Some of you may have been following, as I have, legislation which has been introduced regarding proposed controls over the use of private information. (I happened to see an article in the June 26th issue of Computer World which describes legislation being introduced in the area of privacy.) There are thousands of information files throughout the country--in credit bureaus, government agencies, etc., containing various items of information on individuals. Until recently, I guess there hasn't been a lot of concern over this, because these files have been existing with certain natural "dividers" such as geographic and administrative separation in metal or wooden cabinets; the information has been on paper stuffed in a drawer somewhere; and, usually, the agency that has the information has it for a particular purpose and uses it for that purpose, and only once in a while it's shared.

Things are changing a lot now. With computer data banks, information about you or I which may be collected now or may have been collected ten years ago and is on a piece of paper in that file and can now be put into a computer bank and the information in the computer bank can be collected, can be compiled, can be accessed and very quickly.

Dick Healy pointed out in his presentation on industrial espionage that there are lots of ways to get information. It's obviously more convenient to get at information when it is neatly compiled in a central computer bank. Therefore, computer secrecy is a very important area, and I would encourage the society to address itself to this issue.

I'm always encouraging members of the society to expand their horizons and to get into other areas. I hope we don't channel our vision too narrowly,

and I think that classification managers can and ought to be (and I think many of us are) more than just defense information specialists and Industrial Security Manual specialists. We ought to be concerned with the totality of information protection. Then we are true professionals.

These are some of the things that I wanted to share with you: what we do at SDC and some of the things I think our society ought to involve itself with in the future. Thank you very much.

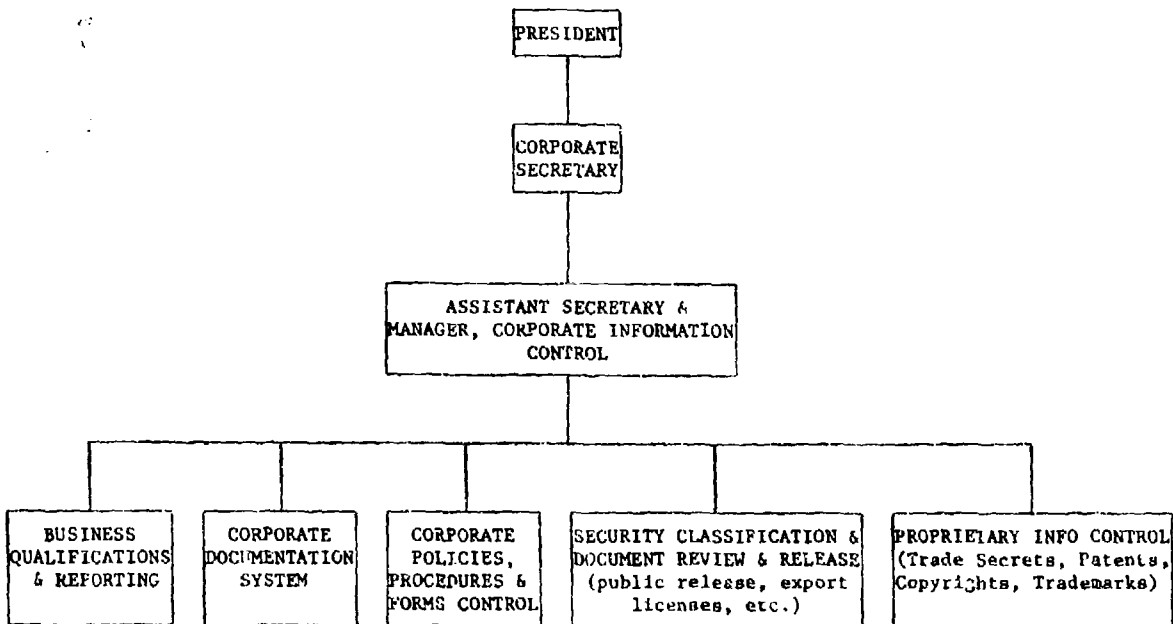


Figure 1

PUBLICATION REVIEW AND RELEASE REQUEST

CLASSIFICATION

- 1. Document No.
- 2. Copy No.
- 3. Date of Request:
- 4. Requester

(See back of form for instructions.)

5. ACTION REQUESTED:

PUBLICATION

- SDC Series
 - Non SDC Medium
 - Oral/Visual Presentation
- Additional Information _____

DISSEMINATION

- Cross-Contract Access
- Outside Release
- Open Publication

CLASSIFICATION REVIEW

- Pre-Publication
- Post-Publication
- Group Assignment

OTHER

- _____
- _____
- _____

6. TITLE (Unclassified)

7. AUTHOR(s):

8. CONTRACT NO. AND PROGRAM NAME:

9. CLASSIFICATION: Military _____ Corporate _____

10. DISTRIBUTION RESTRICTIONS:

| 11. RELEASE TO: Name and Address | No. of Copies | NEED-TO-KNOW |
|----------------------------------|---------------|--------------|
| | | |
| | | |
| | | |

12. DISTRIBUTION BY: Requester Document Distribution Other _____

13. REVIEWS:

| Department | INITIALS | DATE |
|------------|----------|------|
| Department | / | / |
| Department | / | / |
| Security | / | / |
| Military | / | / |
| Other | / | / |
| | / | / |
| | / | / |

14. COMMENTS: Please Initial

15. REQUEST: Approved Disapproved

CORPORATE INFORMATION CONTROL (or DESIGNEE)

Signature: _____ DATE: _____
NAME (typed): _____

CLASSIFICATION

A 1123 (9/67)

4. DEPARTMENT EDITOR'S COPY

Figure 2

TABLE 1. MINIMAL REVIEW AND APPROVAL ON FORM 1125 REQUESTS

| ACTION REQUESTED | MINIMAL REVIEW |
|---|--|
| <u>OPEN PUBLICATION</u> | |
| <ul style="list-style-type: none"> • News releases • Articles for trade newspapers and magazines • General corporate brochures • Corporate advertisements | <ol style="list-style-type: none"> 1) Division/Department/Program Manager 2) Corporate Relations Office 3) Vice President, Corporate Development 4) Vice President, Finance (for financial statements) 5) President 6) Corporate Information Control (CIC) |
| <ul style="list-style-type: none"> • Marketing brochures | <ol style="list-style-type: none"> 1) Division Manager or designee 2) Corporate Relations Office 3) President 4) Corporate Information Control (CIC) |
| Not contract related: | |
| <ul style="list-style-type: none"> • TMs • SPs • Oral presentation and papers • Articles for professional journals | <ol style="list-style-type: none"> 1) Division Manager or designee 2) Corporate Relations Office 3) Vice President, Corporate Development 4) President 5) Corporate Information Control (CIC) |
| Contract related: | |
| <ul style="list-style-type: none"> • TMs • SPs | <ol style="list-style-type: none"> 1) Division Manager or designee 2) Corporate Information Control (CIC) |
| <u>OUTSIDE RELEASE OF INFORMATION NOT CLEARED FOR OPEN PUBLICATION</u> | |
| Contract deliverable: | |
| <ul style="list-style-type: none"> • TMs • SPs • FNs | <ol style="list-style-type: none"> 1) Division/Department/Program Manager or designee 2) Security Office (only if classified)* 3) CIC (for foreign releases only) |
| Not contract deliverable: | |
| <ul style="list-style-type: none"> • TMs • SPs • FNs | <ol style="list-style-type: none"> 1) Division/Department/Program Manager or designee 2) Security Office (only if classified)* 3) Vice President, International Division (for foreign releases only) 4) Corporate Information Control (CIC) |
| Proposals or related materials | |
| | <ol style="list-style-type: none"> 1) Division/Department/Program Manager or designee 2) Contracts Management 3) Security Office (only if classified) 4) Vice President, International Division (for foreign releases only) 5) CIC (for foreign releases only) |

*If address is listed in PIR System, does not require Security Office approval.

Figure 3

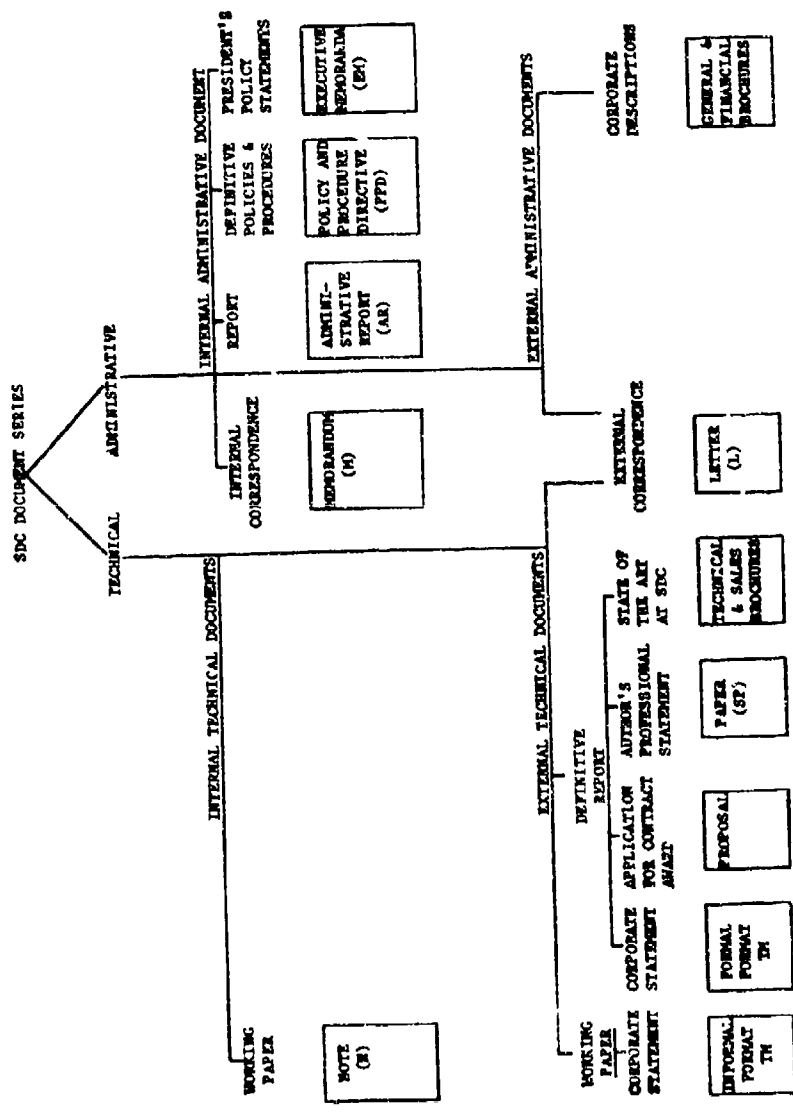


FIGURE 1. OUTLINE OF SDC DOCUMENT SERIES

Figure 4

THIS PAGE IS BEST QUALITY PRACTICABLE
FROM COPY FURNISHED TO DDC

POLICY and PROCEDURE DIRECTIVE

901/210/03

FOR SDC INTERNAL USE ONLY

No distribution or disclosure of this document may be made outside of SDC without the prior consent of an authorized representative of the originating organization.

PROTECTION OF CORPORATE INFORMATION

| <u>Section</u> | <u>Page</u> |
|---|-------------|
| 1. Policy | 2 |
| 2. Applicability | 2 |
| 3. General | 2 |
| 3.1 Corporate Information | 2 |
| 3.2 Document | 2 |
| 3.3 Published Vs. Unpublished | 2 |
| 3.4 Private Vs. Not Private | 2 |
| 3.5 Proprietary | 3 |
| 4. Proprietary Technical and Business Information | 3 |
| 5. Forms of Protection for Proprietary Information | 3 |
| 5.1 Trade Secrets | 3 |
| 5.2 Other Private Information | 3 |
| 5.3 Patent Vs. Copyright | 4 |
| 5.4 Trademark | 5 |
| 5.5 Documentary Vs. Non-Documentary Protection | 5 |
| 6. Controls for Trade Secrets and Other Private Information | 5 |
| 6.1 General | 5 |
| 6.2 In-House Physical Controls | 5 |
| 6.3 Controls for Non-SEC Disclosures | 9 |
| 7. Duration of Protections for Proprietary Information | 12 |
| 8. When and How to Remove Protections | 12 |
| 9. How to Use Table 1, "Protections for Business Information" | 13 |
| 10. Protection of Non-SDC Proprietary Information | 13 |
| 11. The Importance of Keeping Records | 13 |
| 12. Use of SDC Proprietary Information by SDC Employees | 13 |

APPROVED


J. B. Skaggs, Senior Vice President

FILE DATA

Prepared by L. F. McConnell, Corporate Information Control

5 October 1973

Page 1 of 26

This reissue replaces the following PPGs:

- 901/210/02, Protection of Corporate Information
- 901/212/00, Protection of SDC Private Business Information

Material in the above PPGs has been rewritten and consolidated in this PPD. Greater emphasis is placed on trade secret form of protection. Descriptions of patent, copyright and trademark protections are rewritten and expanded. The Patent, Copyright, Disclosure Agreement form (A-1022) is revised to include the business, products, services or projects of subsidiaries.

SYSTEM DEVELOPMENT CORPORATION

QUESTIONS AND ANSWERS

MR. HOYLE: I've got a question for Mr. Bardin.

How much legal protection do we have under what we know of the data protection or the proprietary-type notice which is in all documents?

MR. BARDIN: It serves as an indication of intent and should be considered with other facts and circumstances. If the document is transferred to somebody under circumstances where they know or should know that they are under a confidentiality obligation, that kind of a notice is helpful, but it is not controlling. For example, if you put it in an instruction manual of the type that is distributed freely with an item you sell to a customer, you can put "CONFIDENTIAL" or anything else you want on it and it won't change the character of what otherwise is obviously a disclosure of a nonconfidential nature.

So, in answer to your question, they are certainly helpful in the right circumstances.

On the other hand, this is one of the areas where companies frequently tend to error by often, say, putting such a notice on every single document they send out. In my view, that tends to hamper your ability to protect anything in that it shows that it's merely a formal act rather than a decision that somebody has made on the basis of looking at that particular document and information.

MR. BAGLEY: Mr. Bardin, could you give me the citation on the Supreme Court decision?

MR. BARDIN: The landmark decision is: Kewanee Oil Co. v. Bicron Corp., 416 US 470 (1974).

MR. RICHARDSON: Dean Richardson, TI. Mr. Bardin, before you sit down, let me ask you another question. Have you been following the IBM case that's been going on for the last three years concerning their loss of the patentable information due to this inability or apparent lack of proper handling of their information? Would you care to comment on that?

MR. BARDIN: Well, are you speaking of the litigation with the three hundred fifty million dollar judgment?

MR. RICHARDSON: Yes.

MR. BARDIN: Well, essentially, as I understand that case, the judge acknowledged that he had applied the wrong damage criteria. In other

words, in awarding damages against IBM he really hadn't done it right.

Now, I believe that that award has been corrected to be reduced somewhat, but the case is still very actively involved in appeal and I'm not sure just where it is as far as the loss of rights through inadvertence or otherwise.

I'm just not familiar with the facts enough, really, to comment, and any reliance on the decision would be risky, in that appeal is of course very likely.

MR. RICHARDSON: Thank you.

MR. ARNELSON: Mr. Bardin, Bob Arnelson, Rockwell International.

When we give briefings that contain proprietary data, if the briefing is going to be published, printed, and distributed, it then has an appropriate patent legend or marking put on it.

However, in an oral presentation where nothing is printed or distributed, there is no patent or trade secret restriction put on the presentation, on the premise that you cannot hold a captive audience responsible for acceptance of proprietary information.

Very recently we had a case where an attendee at a briefing being given, which did contain quite a bit of proprietary data, but which is not printed, had a recorder. Under circumstances like that where the information is going to be reproduced--in this case, in that form--would it not be appropriate to make a lead chart or statement implying or stating the proprietary nature of the material?

MR. BARDIN: Absolutely. In fact, one of the things that I try to encourage is that at sales conventions and other conventions, even internal company ones, is that there be a very clear-cut warning statement given that such and such information, which you're going to present, is of a confidential nature.

One of the things that we like you to do if you propose to make a disclosure to a vendor, the ideal situation both from the standpoint of knowledge, alerting him and binding him, is to get him to sign a confidentiality agreement. That is quite common. Vendors will do that in most instances. There are some companies that have a horrible aversion to them. Perhaps some of you represent them here, but it has been my experience that if they want your business

bad enough, if it's important enough, by and large, they will take it in confidence.

Now, conversely, if you have a group of people come into a meeting and you make a sales presentation--particularly if you're the vendor--and you make a sales presentation and you submit the information later on and it's got proprietary information stamp--particularly, the trade secret kind--I don't think that's going to protect you. The vendee is unlikely to know when he is at the presentation that he is under a confidentiality obligation, and unlike the the employer-employee relationship, the circumstances wouldn't suggest it.

So it is a touchy area, and oftentimes you just have to make the disclosure and lose potential trade secret rights, because the business people tell me, "We've got to deal in business and if our legal problem was the controlling factor, we couldn't operate."

LT. COL. JONES: I'm Lt. Col. Jones from the Army Training and Document Command. I'd like to address an area which hasn't been touched on directly and I'd like to address my question to anybody who can answer it.

Within the defense establishment, there are several thousand foreign liaison officers accredited in the United States. They operate under different terms and are allowed access to classified information.

One of my concerns is to see that the information released to the people in the Training Document Command is correct within the regulations. Sometimes it's not always clear. I'd like to know if anyone has any indication that industries in friendly foreign countries have through this means of procurement of information gained any sort of an edge over any of our firms in the world markets for military equipment?

MR. BARDIN: I think they have commercially, but I'm unaware of it through military channels. I might say in that regard, strangely, many foreign countries nowadays are more cooperative and favorable to proprietary rights than we are here in the United States. We have a trade secret-type suit going in England and I've had a little experience in Japan, and, surprisingly enough, they look on it more favorably in those countries, and if there is a problem, I would suspect, without knowing, that it would be easier to cure perhaps than here in our own country. But I have no direct knowledge of information having been acquired through liaison officers.

CLASSIFICATION MANAGEMENT--DIRECT OR INDIRECT COST?

MR. JOHN D. TIPPIT
District Manager
A.B.M.I. Security Services
2145 19th Avenue
San Francisco, California 94116

MR. ROBERT E. BONSON
Senior Member, Contracts Staff
Santa Barbara Research Center
75 Coromar Drive
Goleta, California 93017

PRESENTATION BY MR. TIPPIT

Ladies and Gentlemen, I would first like to express our appreciation to the Program Committee of this, the Tenth National Seminar of our Society, for the opportunity to address you today. This presentation is the by-product of over five years of effort devoted to establishing and implementing a classified information management program at the Santa Barbara Research Center (SBRC). Our program development started about one month after I joined SBRC as Security Officer. At that point I was advised that our present efforts to comply with DOD security requirements were really not what they should be. This advice came in the form of a team inspection which resulted in some twenty seven (27) major and minor deficiencies. Recognizing that prior to joining SBRC I had had very little contact with the DOD program, you can understand why I asked myself, "What have I gotten myself into this time?"

From that beginning in mid 1969, our program progressed to the point where we were nominated and selected for the James S. Cogswell award for 1973. When I speak of we, with respect to the Cogswell award, I refer to the company management which permitted us to implement some innovative procedures; the scientific and operating personnel who adapted their operations to these new procedures; the Santa Barbara DCASR personnel, who did not always agree with our new approaches but were always helpful; and, of course, our security staff. We liked to refer to our efforts as a team effort and later so named our in-house security bulletin. In case you are wondering why I am telling this saga, I feel, now looking back, that one of the most significant accomplishments was the fact that we reaffirmed that the DOD security program can be a workable and an effective program. That's not to say it couldn't stand some improvement; however, we do not need panic changes, in my opinion. I say this primarily after reviewing some of the pending legislation now before the Congress.

I can remember very vividly those first few months when on many occasions I sought guidance and assistance from many of my associates and found abundant help in the areas of physical and personnel security. However, when the subject of retention, DD 254's and such, came up I found mostly negative remarks. Suffice it to say, if I had believed and followed some of those remarks, I would still be trying to explain why we had some 2,000 secret documents without proper retention. It seems to me that we in industry still have not accepted the fact that the Information Security Program is a program which, at least in my opinion, could never be successful as a totally automatic program. It is rather a program that will function effectively only when its designers, practitioners and monitors will remember and follow three basic principles: (1) Nothing is perfect, thus requiring changes now and then; (2) two or three heads are better than one - that's what NCMS is all about; and (3) all change is not bad - give all ideas a fair hearing.

The objectives of our presentation this morning are to (1) share with you the results of our efforts which have led us to recommend the establishment of a direct contract charge relationship for contractor conducted Classification Management activities. We have gone one step further than to just suggest such a relationship; we have identified what we feel could serve as a vehicle for developing this relationship - that being the use of the Department of Defense Data Management Program (DOD Instruction 5C10.12). The operation of this program will be discussed in detail by Mr. Bonson a little later in our presentation, and (2) to recommend the establishment of a joint committee made up of representatives from the National Classification Management Society, the National Contract Management Association and the Department of Defense, to study our proposal in detail and deliver its findings as soon as reasonable.

At this point I will take a minute or two to explain how this idea got started. As mentioned earlier, we had a Classified Information Management Program at SBEC that we were having great success with. Our total program continued to yield deficient free "696" inspections, except for the normal human failures that exist in any program. Then the predictable happened; we had a business slump and, as is normal, we were asked to evaluate our operations for possible manpower savings. I, as did other managers, had to ask myself the question, "What can I cut out? What is really not necessary?" To answer these questions I sat down with my staff and discussed the situation. During the next few days we

found that much of our daily effort was spent on tasks that were not required as part of the DOD program. Most of these efforts involved our procedures for the obtaining, applying and reviewing of classification guidance, as well as negotiating classified material disposition during the contract life. Granted, these efforts did wonders for our program, but when we got right down to it, very little was required. The punch line came when I went to our plant manager and explained the situation. He said, "Let's not change our program, but it would be a lot easier if it was a direct charge program." That statement stuck with me and led to my decision to tackle this project.

My first task was to establish the extent of what a contractor is required to do in the area of Classification Management by his Department of Defense Security Agreement, DD Form 441, and its attachment, the Industrial Security Manual for Safeguarding Classified Information, dated April 1974. The purpose for this being, of course, that as established under Section VI of the DD Form 441, "the Government shall not be liable for any cost or claims of the Contractor arising out of this agreement or instructions issued hereunder." The following is a summary of my findings:

1. Paragraph 5 (General Requirements) establishes the contractors responsible for safeguarding all classified information under his control. Among some of the general requirements included are his responsibility to appoint a security supervisor who is to be responsible for the overall program. Limitation on Disclosure, Safeguarding, Security Briefings, Security Combinations, Public Release and Classified Sales Literature are among some of the other general areas addressed. Of course, in this paragraph we also find the well known 5L (Disposition of Classified Material) and 5M (Retention of Classified Material).
2. In Section II (Handling of Classified Information), paragraph 10 (Classification), it is established that the security classification to be applied to User Agency information will be supplied by the contracting officer or his designated representative. The DD Form 254 (Contract Security Classification Specification) is established as the form to be used for this purpose. We also find the first suggestion that the contractor might be of some help, as the contractor is encouraged to advise and assist in the development of the classification specification in order that their technical knowledge may be utilized and they may be in a better position to anticipate security requirements. Paragraph

10 goes on to establish detail requirements for applying classification to various categories of materials.

3. Section VI, paragraph 60 (Classification Guidance) establishes the prime contractor's responsibilities to provide subcontractor guidance. Of course, this guidance, in most cases, must be approved by the contracting officer.
4. In Appendix 1 (DD Form 254) the proper completion and use of the DD Form 254 is discussed.

The remainder of the I.S.M. is devoted to personnel and physical security requirements and, of course, the proper handling of classified information. In 1971, Colonel George Zacharias stated, "Classification is the beginning and the end of the Defense Industrial Security Program." Colonel Zacharias made another statement in that same speech that I feel none of us should ever forget. "Over classification wastes our resources, underclassification jeopardizes defense."

I believe we can summarize the major requirements thusly; (1) a contractor is required to apply classifications to materials when he can base such action on present or past guidance provided by his customer, (2) once classified, he must handle and dispose of the material as established in the I.S.M. or as otherwise instructed by the contracting officer. I concluded that the DD Form 441 and the I.S.M. would not present a bar to these efforts and felt justified in proceeding.

My second task was to define Contractor Conducted Classification Management Activities, compatible with current government programs. I believe the following will provide a base from which to work.

"Contractor conducted Classification Management activities include those efforts taken to: (1) obtain valid classification guidance and to so maintain such guidance, (2) assist contracting officers in developing appropriate guidance, and (3) insure a continuing effective application of valid guidance."

My third task was to evaluate the restrictions, if any, from the Defense Contract accounting point of view. At this point I punted and asked Mr. Bonson to carry the ball. Bob did so and was able, to his satisfaction, to establish that there were no apparent bars from that side of the fence. However, Bob did advise of the importance of finding an established program to use as a vehicle. We feel we have found that program.

My fourth task was one of satisfying that the program would benefit, assuming this idea was accepted. This was the easiest of the tasks, for I simply reviewed the objectives of the information security program, which in my view are; (1) identify sensitive information, (2) limit access to that information to those responsible individuals who need access to perform their duties, and (3) provide protection only as long as is necessary, so as to maintain the highest level of program integrity. Since I can convince myself that the DOD information security program does not currently fulfill these objectives as I believe they can be fulfilled, I was satisfied that if implemented, our proposal would be of benefit.

I ask each of you to consider what could be more contract related than contract's classification? What can be more important than our nation's defense? We firmly believe that contractor conducted Classification Management activities should have a direct contract charge relationship. We further believe that this relationship would go a long way in removing the "fear of customer" syndrome, which is often the reason given for lack of these types of activities. Further, this relationship would put contractor classification involvement firmly in the proposal stage. It would further provide a realistic base from which industry could consistently assist the government by maintaining a professional and an on going program. And last, but not least, the cost of doing classified work would be allocated to the contract served, not all government work, performed by the contractor.

I would now, at this point, like to turn the program over to Mr. Bonson who will present the real meat of our proposal for your consideration.

PRESENTATION BY MR. BONSON

John and I believe that in order for Classification Management programs to be effectively implemented by Contractors, they should be handled as a direct charge to the contract involved. And why not? As a contract administrator I can tell you that contractors would much rather charge direct to a contract than to embark on extensive indirect efforts that increase the overhead and G&A rates causing the contractor to be less competitive in the market place. In other words, why should all of the contractor's contracts bear a share of the costs of Classification Management, when only a portion are classified contracts?

In support of our beliefs, let me share with you some salient points from the Armed Services Procurement Regulation relative to the definitions of Direct Costs, Indirect Costs and Security Costs:

Direct Costs: Are defined at ASPR 15-202 as "those which can be identified with a particular cost objective, but are not limited to items which become part of the end product as material or labor."

Compare that with the definition of an Indirect Cost at ASPR 15-203: "Indirect costs are those which, because of incurrence for common or joint objectives, are not readily subject to treatment as direct costs." In other words, if it can't be readily identified as a cost directly related to the instant contract, it will be handled as an indirect or "overhead" cost.

By present definition under ASPR 15-205.28, "expenses necessary to comply with military security requirements" are allowable costs to be included in overhead as an indirect charge or--and this is not clearly stated--they can be handled as a direct charge to the contract, if the costs incurred meet the definition on a direct charge.

We believe we have a way to meet both the ASPR requirements for a direct charge, and the Contractor's requirements for implementation on a direct charge basis.

During the initial period after John approached me on the subject of handling Classification Management as a direct charge, the similarity between this type of effort and current Contractual Program Requirements for Quality Assurance, Reliability and Configuration Management could not be overlooked. Each of these program efforts require the contractor--on a direct charge basis--to submit Program Plans and subsequent status reports.

In pursuing this similarity, we reviewed Department of Defense Instructions 5010.12 (Management of Technical Data), 7000.1 (Resource Management Systems of the Department of Defense), and 5000.12 (Data Elements and Codes Standardization Procedures).

It appeared to us after reading these documents that the simplest approach was to create two new data item descriptions pertaining to the submission by the Contractor of a Classification Management Program Plan and the subsequent submission by the Contractor of periodic status reports pertaining to the implementation of the plan.

This would permit the Contractor to charge the contract directly for both efforts and would in essence cover most of the costs incurred by Contractor for his Classification Management efforts. If additional costs were to be incurred by the Contractor for Classification Management that would not be covered in either the preparation of the plan or its implementation, a contract line item (CLIN) could also be negotiated between the Contractor and his customer to cover the specific additional items of direct charge. We will concentrate here, however, on the two data items and their use.

Department of Defense Instruction 5010.12 provides the basic thrust:

1. Under Paragraph IV, Applicability and Scope, it is stated that "The procedures and policies contained in this instruction ... may be used, where appropriate, for all other data such as administrative, financial and program management information ...".
2. Under Paragraph VI, Policies and Procedures, Subparagraph 1, Technical Data Requirements, states that "Personnel representing Program Management, Technical, Financial and other functions shall integrate data requirements in their overall planning. These personnel shall be receptive of the 'data call', to provide the opportunity for including their data requirements in the contractual document."
3. Under Paragraph VI, Policies and Procedures, Subparagraph 3, Acquisition of Data, Sub-subparagraph 3 states "Data products (items) included in the contract data requirements list shall be selected from an authorized data list."

In reviewing the Department of Defense Authorized Data List, dated 1 February 1974, and current revisions thereto, it was determined that no data item descriptions exist relative to a contractor's Classification Management Program Plan or the submission of status reports pertaining thereto. As a result, we have prepared proposed data item descriptions for each of these items. Numbering of each of these data items has been accomplished in accordance with DOD Authorized Data List general information, i.e., Category A (Administrative Management) has been selected because it is most appropriate to the Classification Management efforts we are discussing, and the numbers 4498 and 4499 have been arbitrarily selected to indicate our belief that the data item description should be managed by the Defense Supply Agency who has cognizance over DCAS and its security functions. Another

possibility would be to put the management of these data item descriptions under the office of the Assistant Secretary of Defense with numbering somewhere between 6,000 and 6,099. (The cognizant Government agency for these two data item descriptions should be a matter for investigation and determination during the period in which the overall proposed approach is evaluated).

I have four illustrations to present to you: Figure 1 and 2 set forth the data item description for the Classification Management Program (DI-A-4498). Figure 3 sets forth the data item description of the Status Report, Classification Management Program (DI-A-4499) and Figure 4 (the last) presents a sample contract data requirements list (CDRL) DD Form 1423. This last Figure takes an actual page 2 of a CDRL and adds the Classification Management Program data item and the Status Report data item to show how they might be, under actual circumstances, included in a contract.

It is our belief that both Program Management and the Security Office of the DOD Agency or prime customer will be the ones most interested in receiving, evaluating and approving these data item submissions. It may be that other functions may also be interested and/or have a significant role to play in classification management, and distribution of the Data Item submissions to such additional functions should be specified on the DD Form 1423.

In preparing his response to the RFP/RFQ the contractor sets forth the costs for preparing and submitting each of these data items. It is assumed in this presentation that all direct charges associated with the Classification Management will be covered in preparing and submitting these two data items. However, as we have previously stated, any direct charges not covered should be included in a separate contract line item.

In summary then, we believe we have a reasonable method and approach to handling Classification Management as a direct charge to a contract involving classified hardware and data. This approach does, in our opinion, deserve scrutiny and I join with John in recommending a joint committee be established with representatives from NCMS, NCMA and DOD for the purpose of reviewing and evaluating this approach for possible implementation.

| DATA ITEM DESCRIPTION | | IDENTIFICATION | |
|--|--|---|-----------|
| 1. TITLE | | AGENCY | NUMBER |
| Classification Management Program | | DSA | DI-A-4498 |
| 2. DESCRIPTION/PURPOSE This document serves as the basic documentation of the Contractor's planning of the Classification Management Program to be conducted for the applicable contract items. The plan is used by the Procuring Activity to effect initial review and approval of the Contractor's Classification Management Program and as the basis for monitoring and evaluating the Contractor's conduct of the program. | | 3. APPROVAL DATE | |
| | | 4. OFFICE OF PRIMARY RESPONSIBILITY DSA/I.S. | |
| | | 5. SEC. NUMBER N/A | |
| | | 6. APPROVAL LIMITATION N/A | |
| 7. APPLICABILITY/TERMINATION/REVISIONS This Data Item Description is applicable to all classified contracts. Its purpose is to derive early and continuing Contractor and Procuring Activity attention to the handling of classification and classified requirements on development or production programs with these goals to be established: 1) reduction in the creation of classified data, 2) reduction in retention of classified data, 3) reduction in cost of producing classified hardware or data, and 4) prompt declassification of classified hardware or data wherever possible. | | 8. REFERENCES (NAME OF SOURCE) Industrial Security Manual DI-A-4499 DD-254 | |
| 9. PREPARATION INSTRUCTIONS 1) The Contractor may be required to provide a preliminary Classification Management Plan during the RFP/RFO stage of Procurement. If so, it will follow the general requirements set forth for a formal plan. 2) The Contractor will prepare and submit a formal Classification Management Plan within the period specified in the DD 1423 for Procuring Activity Review and Approval. The Plan shall include: A. Method for review and acceptance and implementation of Program DD 254. B. Plans for briefing Contractor's Program Team of Program's Classified Requirements. C. Implementation of special requirements, ie, Marking, Storage, Visitors, Shipping Procedures, etc. D. Review of possible over/under classification situations. E. Means for reviewing areas of possible reduction of costs on producing classified hardware or data. F. Plan for retention of classified data upon contract completion. G. Compliance with program requirements consistent with the creation of a minimum of classified data. H. Plan for review of Program DD 254 on an annual (contracts up to \$1,000,000) or semi-annual (contracts in excess of \$1,000,000) basis to ensure continued effectiveness and applicability of current guidance. (continued on Page 2) | | 10. WCL NUMBER | |

DD FORM 1664

PAGE 1 OF 2

Figure 1

10. Preparation Instructions (con't.)

1. Plans for implementing A through H above with applicable sub-contractors (first and lower tiers) and Vendors.
3. The Plan shall be prepared in Contractor's own format, organized to meet the criteria set forth above. Distribution of copies of the approved plan shall be in accordance with the DD 1423.

| DATA ITEM DESCRIPTION | CLASSIFICATION CODE | |
|---|-----------------------------------|-----------|
| TITLE | AGENCY | NUMBER |
| Status Report, Classification Management Program | DSA | DI-A-4499 |
| This report keeps the Procuring Activity and other affected activities aware of the progress of the Contractor's efforts in implementing the Classification Management Program. | APPROVAL DATE | |
| | OFFICIAL AUTHORITY RESPONSIBILITY | |
| | FORM REQUIRED | |
| | N/A | |
| Definitive Classification Management Program Plans are submitted by Contractors for Classified Programs. The status reports describes the Contractor's efforts so that the program status can be evaluated. | APPROVAL LIMITATION | |
| | N/A | |
| | REPORTS TO BE SUBMITTED | |
| | DI-A-4498 | |
| PREP. NUMBER | | |
| PREPARATION INSTRUCTIONS | | |
| <ol style="list-style-type: none"> 1) Status reports shall be submitted either annually (for contracts up to \$1,000,000) or semi-annually (for contracts in excess of \$1,000,000) from date of contract award. 2) Status reports shall be in Contractor's format and shall report on the progress made from inception to the first report and subsequently from the last report, in implementing the approved Classification Management Plan at the Contractor's level and at the Sub-contractor and Vendor levels. 3) The last status report to be submitted on the contract shall be a final report covering the period of contract performance including all previous reports (if any), indicating the Contractor's overall efforts and accomplishments in implementing the Classification Management Plan. | | |

DD FORM 1664

PAGE 1 OF 1 PAGE

Figure 3

THIS PAGE IS BEST QUALITY PRACTICES
FROM COPY FURNISHED TO DDC

| ITEM NO | | TO SUBJECT | | SYSTEM | | CONTRACT DATA ELEMENTS LIST | | CATEGORY | | CONTRACTOR Santa Barbara Rs Ctr | | DISTRIBUTION AND ADDRESS | | |
|---|-----------|-----------------------------------|----|--------|--------------|-----------------------------|---------|----------|---|---------------------------------|-------------|--------------------------|-------|------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | |
| A005 | DI-F-1708 | Section E of Schedule | LI | 0 | ASSEL-NV-FIR | ASSEL-NV-FIR | One/2 | 30 DAC | As re-quired, with Revisions. | Security Of- fice | Pt. Belvoir | 2/0 | | |
| A006 | DI-A-4498 | Classification Management Program | LI | A | ASSEL-NV-FIR | ASSEL-NV-FIR | 180 DAC | 180 DAC | Annually thereafter, final due to DA contract completion. | Security Of- fice | Pt. Belvoir | 1/0 | | |
| <p>NOTE: THIS IS NOT ACTUAL CDRL FROM A CONTRACT. IT IS A SAMPLE PREPARED TO SHOW HOW A CDRL MIGHT APPEAR WITH THE TWO DATA ITEMS INCLUDED.</p> | | | | | | | | | | | | | TOTAL | DATE |
| | | | | | | | | | | | | | TOTAL | 3/1 |

Figure 4

QUESTIONS AND ANSWERS

MR. HOYLE: Jim Hoyle, Lance Project, Office of Huntsville, Alabama.

I'd like to direct a couple of questions, if I may, to Mr. Bonson.

I am prefacing my remark by an old saying, "Many times it's better to remain silent and be thought a fool than to open your mouth and remove all doubt."

However, I do seek knowledge. That's one reason I come to these seminars. As we gain knowledge, we get smart.

On your proposed data item list, I have to put myself on the other side of the fence. To me, in one respect, it was like some wasted effort. Number one, in a User Agency the directive is given by a DD Form 254 to the contract force.

It's never stagnant. It is changed at least once a year. Normally, in the downgrading area.

In the ten years that I've worked on the DD 254 for our project, for example, we have consistently downgraded and declassified more and more information. Now, granted, there are certain supersecret projects and so forth in which your data items might be beneficial, but for the regular run of the mill type, I just can't see it. It appears--and I'm on the other side of the fence now--it appears that the contractor has found another method in which to make money. Were I in his shoes, I'd do the same.

Develop a proposed data item for the security management program--This is fine. I feel--My feeling, rather, would be that whatever the contractor desires to do in carrying out a program of security classification management is his business. We give a direction. We have the DCASR to do the monitoring, and whatever the contractor needs to do or has to do in order to carry out those orders is his business, so I'll be on the other side of the fence in the beginning in not recommending the data item.

I work in the same office with the man who does the data item. I just can't see it.

MR. TIPPIT: Before your question, let me comment on your statement.

Recognize, as you do, since you're familiar with the data item description, that there is no requirement for the contracting activity to implement it in every contract, and since all of your

programs are so appropriately classified, you would not have to implement it, and it is a negotiable item, so if in your activity you did not feel the necessity of implementing this data item description, certainly as a contracting officer, you would have the opportunity.

MR. BONSON: Even greater than that, the Government is getting the advantage in your method of having to cost--for doing what you say is being done--spread over all contracts, and I submit that there are a great many customers who wouldn't want that charge to be included in the overhead for a nonclassified program. Why should he bear the cost for something he is not getting any advantage on?

MR. HOYLE: Right, I concur with that to make a direct cost. You take one company performing on many contracts known as one classified, it is logical to make a direct cost for that contract. I agree with that.

My question was this: Has this been implemented with Fort Belvoir?

MR. TIPPIT: No.

MR. BONSON: No, we've merely used Fort Belvoir as an example on the Form 1423. I chose to show how it might be implemented on a typical 1423. In no way have we discussed this with Fort Belvoir.

MR. TIPPIT: Next question. Yes, sir.

MR. BOWERS: Bud Bowers, Westinghouse, Annapolis, Maryland.

I have a double-barrel question for you.

First of all, how do you determine in your proposal effort what the costs are going to be? Is it like a percentage, or is it a factor of so many dollars, for basically the same effort goes into a large contract as it would into a small one?

The other part of the question is since I have somewhat of a contract background, I anticipate that most of these people are going to find resistance from the contract people when they go to do this, but how do you--I lost my thought.

MR. BONSON: Well, your question was, basically, how do you happen to handle this type of thing, and my answer is very similar to the way you would handle quality assurance program plans, reliability program plans, configuration management program plans. I think you can argue that

each of those should be an indirect charge, and, in fact, they used to be, but the idea of getting a quality/reliability program at a high level, shall we say, rather than quality, but a high level configuration management program attendant to the needs of a contract, they all come around to having data item descriptions established for them, and to being direct charges in a contract, and being required at the RFP, RFQ stage.

How do you identify the costs that go along with that is along the same route as how do you identify the costs for a quality assurance program plan. You have quality assurance in every one of your companies. If you're on industry's side of the house, you have a quality assurance department, but the program plan sets forth something that the Government wants to know, or the customer wants to know, how you're going to handle specifically the quality on that particular program, because they have found that contractors are inconsistent.

Let's face it. Your company is different than mine. And ours is different than somebody else's down the street as far as implementing quality, reliability, and configuration management. Hence, the customer, more specifically, the Government, says, "Hey, we want to see what it is," and it may not have to be the same for every program.

This program may be unique, and that gives the program office of the customer an opportunity to review that particular program and say, "Yes, this one I want to implement."

I think one of the points I want to address with regard to classification management program planning is that contractors will take the DD 254, will review it, and they will exert various levels of implementation of that DD 254.

Now, John--The program that he and I have worked on and what we've done with our particular program became, I think, very significant because we have gotten the program manager in early and on a continuing basis to take a look at the problems of classification management on a particular program.

We have had study programs as well as reproduction and production programs. I can tell you with regard to the production program, we have had some significant reductions in cost by appraising the program management team of how to handle it in regards to the DD 254. For instance, manufacturing, when you start to put together some assemblies, if you were to follow the DD 254, in

some cases, you would have a classified assembly at a very, very low level, and I can also tell you that's expensive from a manufacturing standpoint.

We have figured out ways to reorganize our production programs to handle the subassemblies to a point that they don't get classified until a much later time, and the costs associated with all that are pushed aside, because we don't have to pass those on to the Government.

We have been able to get back to our customer on an active classification management basis, and actively worked the problem of classification management of the DD 254 to reduce the cost to them and to ourselves.

MR. TIPPIT: I might add to that, too, by the way, that, again, the fact that your company--our company and some other company does have a different approach to classification management, at least in my view, should not be considered bad.

I think sometimes you can systematize the effectiveness right out of the program, and I think the innovativeness of the professionals in this business should be allowed to be expressed, and that expression could take the form of that company's particular classification management program plan, and recognizing that the CO would continue to have the opportunity to approve and negotiate the conditions of that plan.

MR. BONSON: Or to determine if it was even required to start with. We're providing a vehicle for those customers and those agencies that want to implement something more than just routine or haphazard classification management on a program.

MR. BOWERS: The latter part of my question is if you have a large number of contracts, would this not be almost an accounting burden to keep track of the hours and time that were expended for classification management on a huge number of contracts?

MR. BONSON: Not any more than it would be for a program manager who splits his time between a number of different programs, and I think most of our companies on industry's side have that kind of a situation where you don't have a program manager exclusively assigned to one program, and he splits his time on numerous programs, and he splits his time up on his time that way.

Also, with regard to, say, the quality assurance. If you have him referring back to quality, reliability and configuration management in the preparation of the program plan, it's certainly a

direct charge, because they know how much time they spent in preparing that plan, and you also know that they're putting into that the cost of doing all the research and the engineering work, and everything else that goes with it, so that the costs can be isolated, and quite effectively. It also reduces your overhead.

MAJOR CHERRY: I'm Major Cherry. I'd like to speak not as a customer because our organization has a hundred and twenty-two contracts out with a number of you folks and plus some more--

MR. TIPPIT: We need more. (Laughter.)

MAJOR CHERRY: Okay. I'd like to show you, I think, maybe how as classification managers you can write some of this off as a cost of a classified contract as opposed to a cost of your normal overhead.

At FTD, my alarm system alone is now about a four hundred thousand dollar arrangement. We've got a thirteen and a half million dollar expansion program on alarm systems. To cover that, it's going to cost a million two hundred thousand.

Now, that I can't really charge off, so let's say our exploitation and make it twenty-five. Okay, but if you take and figure out how many secret documents you have to maintain and how many confidential documents and how many linear footage in different types of safes, remembering now that a confidential document doesn't require the same degree of protection of secrets and so forth, you could, I think, very legally, very justifiably, show your contract monitor, "Hey, I happen to have 'X' number of safes just to cover your contract." Now, this isn't going to help against the guard force or your alarm systems or the types of vault doors you happen to have, but it's going to help a lot, I would think.

MR. BONSON: Well, may I suggest this, that what we're talking about is just a little different than what you're talking about in regards to alarm systems, safes, and so forth.

Those types of costs fall into your plant itself, the physical plant, and facilities, and on the DD 254, there's a block down there in that DD 254 that says if it's over and above the requirements of your agreement with the Government, then those costs are allowable costs and additional costs.

What we're talking about here, of course, is a different thing. It's classification management

itself, not the plant protection. Plant protection under ASPR 15208 is an allowable and allocable charge.

MAJOR CHERRY: You will find that you will increase your clock with your management though if he figures out that about twenty-five percent of his cost is going for security. Most of the managers don't realize that, and if you can come up with what your costs are in your individual organizations, you may just find yourself able to--

MR. BONSON: You'll find no disagreement from us on that.

MR. TIPPIT: I really wonder--and as I hear you speaking, I'm in tune with you--but I think really the thrust of our considerations here is not the cost being the No. 1 item. What we are saying is that traditionally in industry the thing that's made us get off our duff and get behind a program is a direct charge relationship.

Now, the gentleman over here who indicated that in his opinion this might be a way of making money, well, I'm not sure of that. I'm not sure that that would be a way of making money, but I do know it would be one way of improving a lot of the weaknesses that now exist in the program.

They're not written in there, but they are there and I think both of us on industry and Government can agree on this.

Yes, sir.

MR. LARSEN: Frank Larsen, CNO. A comment to John Tippit on a statement you made during your presentation.

It was refreshing to hear your sense of priorities about the information security program, and to paraphrase, when you said, first of all, to identify, and then, secondly, protect that which is truly sensitive in the national interest.

We in the Navy feel that that is the sense of priority because this is a security program, and working together all of the other concerns and nuances we hear about the information security program will take care of itself. I congratulate you on your sense of priorities.

MR. SUTO: Gene Suto, President-elect of NCMS.

First of all, I want to say that NCMS will be very pleased to work with you on this particular area.

Secondly, we've already been doing some work in this particular area that we will send to you in the very near future. This is in connection with the DD 254 and the contractor's participation in the DD 254.

To address the gentleman's question over here, it's fine if you have a User Agency giving you all this wonderful detailed classification guidance as you're doing, and you're to be complimented, but--

MR. BONSON: This is one of the better program offices. That's for sure.

MR. SUTO: -- we have found that there are many, many contractors around the United States who are getting little or no classification guidance, and if the contractors are given this opportunity to develop this guidance, plan, and furnish it back to the User Agency, we will all be better off and have a more viable program, so I think these gentlemen are to be complimented for their concept.

MR. BONSON: I wish the Lance program office had some way of talking to the rest of the DOD agencies how it's done, because we don't get that kind of support from all our customers. I don't have any contracts with him, apparently.

MR. TIPPIT: I know. That's what you're trying to develop. (Laughter.) The many of you who have been involved, as I have, in offensive intelligence, I think you can remember and recognize that one of the most effective aids to the offensive intelligence community is the existence of confusion in the defensive operations of the, you might say, target.

I suggest that we have a bit of confusion in this program that is being used significantly by offensive intelligence agencies, be it that of the Army against the Navy, or what have you, (laughter), but, at the same time, I would like to say that again we do not have all the answers here in our proposal. We do not even think about coming up with all the answers, but we do feel that this could be a viable program and we feel that the data item description, although it may not be the perfect vehicle, may be the vehicle to get us on the track and subsequently, DOD might have another vehicle in mind.

So unless there's any other questions or comments--

MR. BONSON: There's one back here.

MR. TIPPIT: We still have about ten minutes.

MR. LEYTHUM: I'm Gene Leythum, Boeing.

I know some of your comments are valid, but I think there's also some pretty unsurmountable problems you get in a corporation such as ours-- multiple facility and multiple usage.

We've found it's most efficient to centralize a lot of our operations such as in our data files. Our security operations are important operations and it becomes quite an extensive accounting procedure to try to identify some of those costs out to a specific contract. We've been looking at some quite some time and we haven't been able to come up with a way where you can satisfactorily identify it solely to a specified contract.

The best we've been able to do is identify certain apparent items to a contract, and others to indirect costs of overhead.

In my office alone, for example, I have the responsibility of all classified programs. I would have to hire extra people, and if I kept records of how much time I spent supporting an individual program, it would carry from day to day.

We run into the same thing with our security guards. We utilize a lot of our facilities on a shared basis, so that the program may come into a facility only in a manufacturing area, so I can use it only a portion of the time. To try to figure out how much of that security guards time is allocated to that program--

MR. BONSON: Sir, let me stop you right there, because I think the point you're making is a valid point, and, for that very reason, we would not ever anticipate trying to allocate physical security, either manpower or facilities, against contractors. Again, this proposal is limited to those activities which would directly relate to the classification determination and application on a contract.

MR. TIPPIT: Definitely not physical security; definitely not covered at all. We're talking strictly about that function having to do with classification management. I tend to agree with what you're saying if you have it on the corporate level. I think there's a number of ways to handle that from an accounting standpoint, however.

The least resistance for your particular case would be to say not separately priced. It's included in overhead.

MR. TIPPIT: And I think another thing that you could consider is that--as Bob pointed out to me earlier in the contract management field development, when many of these overhead programs made the shift--some of the same comments that have been made here today--

MR. BONSON: What do you do with quality assurance at the top level? Most of the QA directors report at a pretty high level in the company, and the Government wants them that way. The customers want quality assurance now, and you're staffed with some pretty high level people and costs, but yet we are able to effectively isolate the costs of preparing a program and implementing a specific program for a particular contract.

MR. TIPPIT: I would suggest, frankly, that the implementation of a direct charge classification management program would really not even come close to the magnitude of the quality assurance, the configuration management, or such type of an item.

MR. BONSON: We could show those for similarity of background and purpose rather than similarity of cost.

MR. RICHARDSON: Dean Richardson, TI. Somebody said to me the other day, "Boy, you got a question for everybody, Dean," and I don't really have questions. I'm just curious about a lot of the things that are said up here, and I'm particularly curious about this very innovative approach to handling the costs or even just getting--and a lot of contractors have this very serious problem--about getting a bill, because somebody has to pay for that guy, and how is the company going to afford additional overhead for a classification management position?

This is a good approach.

Now, let me ask you this. What has been your track record on acceptance by your customers, as I kind of get the feeling you haven't really done this yet.

MR. BONSON: We have been doing everything but getting it on a direct charge basis. This is the first time we've presented the idea of direct charge to anybody. We felt this was the best body to present it to to get a reaction. I am pleased to see that the NCMS people are willing to participate in it.

MR. RICHARDSON: You haven't approached any customers with this till--

MR. TIPPIT: Well, recognize that our program was implemented at the Santa Barbara Research Center. We would have probably never gotten to this point, really, because we were very satisfied and having a tremendous success with our customers in terms of the applications of our program, but when that inevitable question was asked by the boss, "Hey, what am I paying for? Is it required by the Government," I had to say, "No, it's not," and except for the foresightedness of the management at that particular facility, I think many managements would have said "Well, sorry, Charlie, but you've got to cut your classification management in two," and I think to the detriment of the program, so it was this realization, I think, in my own mind that led me to discuss the responsibilities with Bob, and got us here today.

MR. BONSON: The second part of the answer to that is yes, we're going to try.