

9314478

UB
247
.A2

R E P O R T

T O T H E

S E C R E T A R Y O F D E F E N S E

B Y T H E

C O M M I T T E E

O N

C L A S S I F I E D I N F O R M A T I O N

NOVEMBER 8, 1956

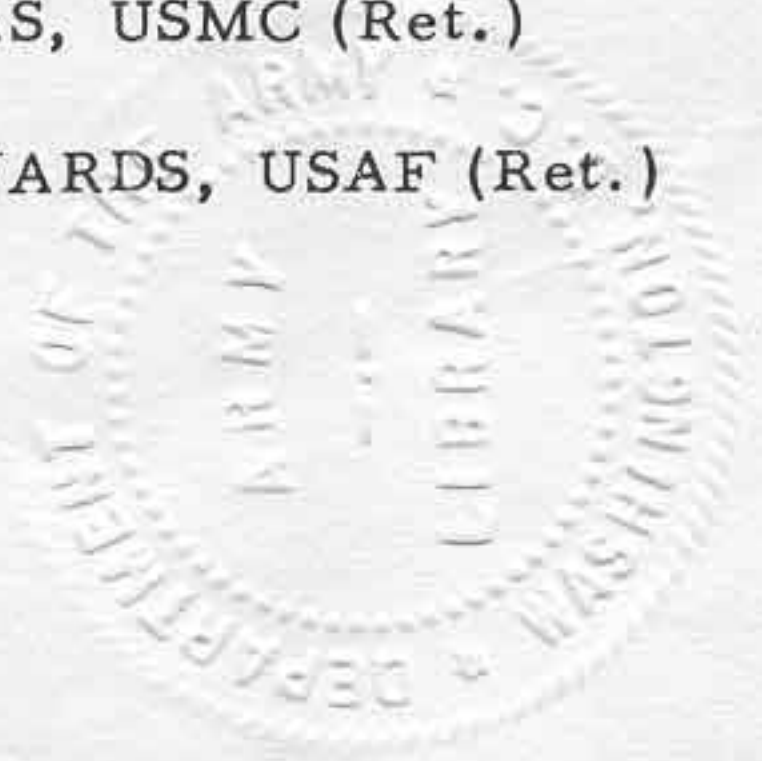
CHARLES A. COOLIDGE, CHAIRMAN

ADMIRAL WILLIAM M. FECHTELER, USN (Ret.)

GENERAL JOHN E. HULL, USA (Ret.)

GENERAL GERALD C. THOMAS, USMC (Ret.)

LT. GENERAL IDWAL H. EDWARDS, USAF (Ret.)



T A B L E O F C O N T E N T S

	<u>Page</u>
I. Difficulty of the Problems	1
II. Scope of Activity	1
III. Basis for Classification	1
IV. Operations of the Classification System	2
A. Overclassification	3
B. Unauthorized Disclosures	6
V. Fundamental Causes of Shortcomings	8
VI. Recommendations on the Two Major Shortcomings	10
A. Overclassification	10
Recommendation No. 1	10
Recommendation No. 2a	10
Recommendation No. 2b	11
Recommendation No. 2c	11
Recommendation No. 2d	11
Recommendation No. 2e	11
Recommendation No. 2f	12
Recommendation No. 2g	12
Recommendation No. 2h	13
Recommendation No. 2i	13
B. Deliberate Unauthorized Disclosure	15
Recommendation No. 3a	15
Recommendation No. 3b	16
Recommendation No. 3c	16
Recommendation No. 3d	16
Recommendation No. 4a	17
Recommendation No. 4b	17
Recommendation No. 4c	17
VII. Unauthorized Disclosures of Administrative Matters	18
Recommendation No. 5a	18
Recommendation No. 5b	18
Recommendation No. 5c	19
Recommendation No. 5d	19

	<u>Page</u>
VIII. Industry	19
Recommendation No. 6a	19
Recommendation No. 6b	20
IX. Congress	20
Recommendation No. 7	21
X. The Press	21
Recommendation No. 8a	22
Recommendation No. 8b	22
Recommendation No. 8c	22
XI. Concentration of Implementation	23
Recommendation No. 9	23
XII. General Conclusions	23
XIII. Summary of Recommendations	23

Tab A	Terms of Reference of the Committee on Classified Information dated August 13, 1956.
Tab B	Executive Order 10501 dated November 5, 1953, Subject: Safeguarding Official Information in the Interests of the Defense of the United States.
Tab C	Department of Defense Directive 5200.6 dated June 1, 1954, Subject: Policy Governing the Custody, Use and Preservation of Department of Defense Official Information Not Within the Purview of Executive Order No. 10501.
Tab D.	Department of Defense Directive 5230.12 dated March 27, 1956, Subject: Release to the Public of Information on Guided Missiles, Military Aircraft, Associated Powerplants, Components and/or Accessories.
Tab E	Remarks of Dr. Vannevar Bush, former Chairman, Research and Development Board, before the American Society of Newspaper Editors on April 16, 1948.

REPORT OF
COMMITTEE ON CLASSIFIED INFORMATION

To The Secretary of Defense:

The Committee on Classified Information which you appointed on August 13, 1956, and charged with the duties set forth in a letter of that date to its Chairman (a copy of which is attached as Tab A), submits the following report.

I. Difficulty of the Problems.

It is an understatement to say that the problems you have confided to us are not easy. They are of long standing and have not yielded satisfactorily to real attempts to solve them in the past. Your Committee therefore has been under no illusion that a simple corrective formula could be found.

II. Scope of Activity.

We have conferred with personnel in your office and in the military departments who are primarily concerned with information security, with the civilian and military heads of the military departments, with the Chairman of the Joint Chiefs of Staff, with representatives of other government agencies whom we thought might prove helpful, with representatives of the press, and with certain other individuals totaling in all approximately fifty persons. We found without exception an attitude of complete cooperation and helpfulness.

III. Basis for Classification.

At the risk of stating a platitude, this country is far different from a dictatorship, and the impact of that difference is strong on the problem of information security. Being a democracy, the government cannot cloak its operations in secrecy. Adequate information as to its activities must be given to its citizens or the foundations of its democracy will be eaten away. We find that the Department of Defense fully subscribes to these principles. On the other hand, our democracy can be destroyed in another way, namely, by giving a potential enemy such information as will enable him to conquer us by war. A balance must be struck between these two conflicting necessities.

In the Department of Defense there are peculiar factors which make the striking of the proper balance difficult. The Department spends roughly two-thirds of the national budget. At one time or another it directs the lives of millions of our young men and women. And it is charged with planning for the survival of the nation in case of war. These considerations center public interest on its activities and weight the balance in favor of maximum disclosure. On the other hand, the activities of the Department are of the greatest interest to a potential enemy. He can profit from disclosures of its activities to a far greater extent than disclosures of the activities of most of the other governmental departments. So the other side of the scales is heavily weighted. The result is that striking the proper balance is more important and more difficult than is the case with most of the other departments of the government.

The principal document governing the determination of how to attain the proper balance is Executive Order 10501 (attached as Tab B). This Order recognizes the principles outlined above by prescribing a dual objective (1) to give the public full information up to the point beyond which national security will be damaged, and (2) to protect information beyond that point. This protection is given by controlling the circulation of sensitive information so that recipients will be confined to persons who have been determined to be trustworthy and who have a need to know the information in order to perform their duties properly. Obviously this entails the establishment of mechanics to identify sensitive information so that all will know it should be protected. Further, since some items of information are more sensitive than others and so need more careful handling, the procedures should grade information according to its sensitivity. Accordingly, Executive Order 10501 prescribes that sensitive information should be classified in three categories - "TOP SECRET," "SECRET" and "CONFIDENTIAL," and further prescribes the degree of protection applicable to each category.

All this seems to us beyond reasonable criticism as a matter of theory. No one has suggested to us a better system. Indeed no one has been able to suggest any other comparable system.

IV. Operations of the Classification System.

It is, however, one thing to have a theoretically sound system and quite another thing to make it operate well in an enormous organ-

ization such as the Department of Defense. While we commend the operation of that part of the system which deals with enforcing regulations covering the physical safeguarding of classified information, we feel that in certain other respects the system is not operating as well as it should. The Department of Defense is accused of failing to accomplish both of the dual objectives of the system: it withholds too much information and too much leaks out. We think both criticisms are justified; there are both overclassification and harmful disclosures.

A. Overclassification.

The fundamental difficulty in the problem of overclassification is that the criteria for determining whether information should be classified at all, and if so what degree of classification it should bear, are necessarily general. If the damage to the nation which a disclosure of defense information could cause is exceptionally grave, the information should be classified as "TOP SECRET"; if serious, "SECRET" is the proper classification, and if the disclosure could be merely prejudicial to the defense interest of the nation, then "CONFIDENTIAL" should be used. While some examples of the first two categories are given as guidelines, they are largely confined to the effect of disclosure on international relations and the definitions themselves remain general and therefore vague. Two reasonable men of similar background and possessing equal knowledge could well disagree on the application of these criteria to a particular piece of information. When it is realized that within the world-wide activities of the Department of Defense hundreds of thousands of individuals must be authorized to apply these criteria in at least the Confidential category, it is not surprising that the results are often inconsistent. Within certain technical areas guides for classification have been provided, and the Air Force has made an attempt to supply general guidance in applying the criteria. We commend these efforts, but the problem of generality of the criteria is still a major one.

There are other factors which aggravate the situation. A subordinate may well be severely criticized by his seniors for permitting sensitive information to be released, whereas he is rarely criticized for over-protecting it. There is therefore an understandable tendency to "play safe" and to classify information which should not be classified, or to assign too high a category to it. The use of even Top Secret has gone far beyond that contemplated in Executive Order 10501. While the infor-

mation protected by this overclassification is not as a rule important for the public to know, the resulting load impairs the functioning of the system.

Further, there is a tendency to use the classification system to protect information which is not related to the national security. Perhaps the prime example is information dealing with administrative matters. We strongly believe that, even though the Department of Defense is a governmental agency and cannot expect to operate with the privacy of a business organization, there are nevertheless certain matters which if made public would reduce the efficiency of the operations of the Department below the standard which the public itself requires. Personnel records is perhaps the most frequently cited example of this type of information. An example of equal or perhaps greater importance is papers expressing the views of the staff to superiors. If these papers are not held private, then the written advice of staff members to their superiors may be such as they think will later look well in the public print rather than their true opinion. But granted the necessity for protecting these administrative matters, such protection is justified on other grounds than the national security. Within the Department of Defense it is covered by Directive 5200.6, (Tab C), which requires among other things that "preliminary documents relating to proposed plans or policy development" should not be disclosed "when disclosure would adversely affect morale, efficiency or discipline," and which authorizes the use of the stamp "FOR OFFICIAL USE ONLY." Nevertheless there is a marked tendency to classify this information under Executive Order 10501. This constitutes an abuse of the classification system established by that Order and tends to destroy public confidence in the system.

We have heard allegations as to another type of abuse of the classification system, namely its use to cover up administrative mistakes. We have found no instances of such abuse, and believe that if it exists at all it is of minor importance in the problem of overclassification.

There is, however, another real source of overclassification. It is the attempt to do the impossible - to keep as classified information which can no longer be withheld. The physical appearance of a test model of a new plane which must be rolled out of the manufacturer's plant adjoining a public highway is an example. General performance data of a new plane which has become widely known prior to quantity production is another. Information originally classified and subsequently officially revealed and the classification of compilations of unclassified data are other examples.

Still another aspect of overclassification is the use of the system to protect information which ordinarily would be released but which is withheld temporarily in support of a foreign policy objective. Whether or not this is overclassification in the strict sense of the word, it is certainly so regarded by the press, and it is disturbing to the system. Granted that standards of what is harmful to the national security should vary with the international situation and so be generally responsive to foreign policy, the system cannot be operated as if steam were being turned on or off in a radiator. Rather the system is like a hydro-electric dam where the water can be gradually raised or lowered, but not suddenly. There are too many people involved for sudden shifts of policy. Confusion, uncertainty and loss of confidence in the system result.

Theoretically overclassification can be remedied by declassification. And Executive Order 10501 contains admirable provisions relating to declassification. These provisions are not, however, working satisfactorily. In only a few offices is declassification keeping up with the creation of current classified material, and the backlog of classified information created during and since World War II remains substantially untouched, in vaults, warehouses and industrial plants. While we do not consider that dissolving this backlog would contribute in a major way to the immediate problem of safeguarding current classified information, we do feel concern over the failure to keep up a declassification program on a more current basis. The Executive Order requires that where possible a date for automatic declassification be set at the time of classification. This device is not widely used, largely because of reluctance to rely on forecasting future events. Probably it could and should be used more widely. But even so, there is a great field where it cannot be applied. Current practice is to consult the office which originated the classification before declassifying. This entails an appreciable amount of paper work. Further, when the document is declassified notification must be given to all those who have copies, which often entails a formidable task of additional paper work, especially where industry is involved. With the continuing requirement to reduce administrative personnel throughout the Department of Defense, the additional effort and paper work necessary to attain adequate declassification has simply not been forthcoming. The act of classification is simple and expeditious, declassification is involved and tedious. In the battle between the two, the advantages are on the side of classification, and declassification has fallen below the effectiveness envisaged by Executive Order 10501.

For all these reasons overclassification has reached serious proportions. The result is not only that the system fails to supply to the public information which its proper operation would supply, but the system has become so overloaded that proper protection of information which should be protected has suffered. The press regards the stamp of classification with feelings which vary from indifference to active contempt. Within the Department of Defense itself the mass of classified papers has inevitably resulted in a casual attitude toward classified information, at least on the part of many.

B. Unauthorized Disclosures.

The seriousness of unauthorized disclosures, both in number and nature, cannot be determined, because only those which come to light are available for evaluation. The unknown ones are probably the most vicious in that they are likely to include those involving real espionage. We can only hope that there are not many of them. It is, however, obvious that the weaker the protective system is, the greater the number of unknown compromises will be. This of course is a reason for our concern over the factors described in connection with overclassification which tend to weaken the system.

As to known unauthorized disclosures, not all are serious. The number and nature of those which have been traced to careless violation of the rules for physical protection (locking safes, manner of transmission of classified information, etc.) persuade us that the violations of these rules within both the Department of Defense and industry is reasonably under control. Nor do we think that unauthorized disclosures occurring at social gatherings, either through carelessness or to enhance someone's ego, as distinguished from deliberate "leaks" considered below, present a serious problem. While it is true that compilations of data which are composed of unclassified items may disclose information helpful to a potential enemy, their disclosure in all probability merely saves him some time and effort, and does not appear to us to represent a major problem.

We are, however, concerned with deliberate disclosures of classified information or so-called "leaks." While in many cases it could be argued that the information so disclosed is not really of serious security significance, that is not always true, and these leaks evidence a breakdown of the system and indeed of discipline itself which, if unchecked, may have most serious consequences. There have been a good many instances of this type of unauthorized disclosure over a considerable period of time, and the number appears to be increasing.

Due to the difficulties in identifying the sources of these leaks because of the large number of persons who have had access to the information in question, it is impossible to describe with certainty the individuals who are responsible and the reasons which motivated them. We are, however, left with the strong impression that both civilians and military of considerable position and rank are involved, and that they are generally motivated by a desire to further the interests of a particular Service.

There is no doubt that the traditional differences in point of view of the three major Services are accentuated today. The revolutionary developments in new weapons since the advent of the atomic bomb have made mandatory a continuing review of the over-all concept of national defense, to determine how to spend most wisely the money which our economy can afford for national defense in this indeterminate period of strained international relations and rapidly developing technology. Further, it is not possible to demonstrate that the decisions of these difficult problems are right when taken. The decisions involve a balance of calculated risks, on which reasonable men may differ. Only a war can prove whether the decisions are right. Under these circumstances it is understandable that different Services will have different concepts and that ardent advocates of a particular concept will wish to do everything they can to weight the balance in favor of their particular philosophy. The deplorable thing is that they should carry their ardor to the point of undermining the system on which the nation relies for the protection of its defense secrets and should flout the discipline which makes all the Services, their own included, effective.

In this connection, it is doubtless true that loyalty to a Service has a greater appeal to the individual, since it is rooted in years of tradition, then does loyalty to the comparatively recently created Department of Defense. Also, when one Service has apparently profited by taking its case outside the Department, the pressure to obtain a similar advantage for another Service is intensified. But in our judgment neither of these considerations is an excuse for excesses which damage the whole defense effort.

Nor is there any excuse on the ground that when there is disagreement among the Joint Chiefs of Staff, decision is made by the Secretary of Defense and a few non-military advisors. Some members of the press appear to think that this is so. On the contrary, the Secretary

of Defense can and frequently does obtain the advice of the Armed Forces Policy Council, composed of the Secretary of Defense, the Deputy Secretary of Defense, the Secretaries and military Chiefs of the three military departments and the Chairman of the Joint Chiefs of Staff. If agreement is not reached in that manner, the matter can be and often is taken to the President or presented to the National Security Council, chaired by the President, where dissenting views can be fully heard. Even after a matter has been heard at the National Security Council, appeals can be and sometimes are made to the President. In our view the refusal of members of a Service to accept decisions reached after such a process is utterly inexcusable.

From the foregoing we conclude that the two major shortcomings in the operation of the classification system are overclassification and deliberate unauthorized disclosures. We further conclude that little, if any, progress can be made without a successful attack on these two major shortcomings.

V. Fundamental Causes of Shortcomings.

Preliminary to suggesting remedies to defects in any given situation, it is often profitable to inquire into their causes, in an endeavor to identify the fundamental ones and so make remedial action simpler and more effective. In our view, the trouble in this case does not stem from defects in statutes, executive orders, directives or regulations. No change in the statutes or executive orders has been suggested to us which would in our judgment contribute significantly to improving the situation. The directives and regulations seems to us to be in the main well conceived and conscientiously administered by the security offices both in the Office of the Secretary of Defense, in the Joint Chiefs of Staff and in the military departments. While they may need supplementing to carry out some of the recommendations in this report, they are not the cause of the trouble. The trouble lies deeper than that.

We have been told that information security is a state of mind and not a set of rules. With this we agree. We further think that a state of mind is part of morale, and as such is a facet of discipline, and discipline is a command function.

Stating the matter less abstractly, a failure to comply with the regulations governing information security is a breach of discipline as

much as a failure to comply with regulations for the proper maintenance of weapons. It is immaterial whether the failure is inadvertent, as is generally the case in overclassification and in some unauthorized disclosures, or is deliberate, as in the case of disclosure to further a particular military concept.

Generally speaking, it is very difficult in this country to enforce compliance with rules if those rules are not widely accepted as both necessary and reasonable. The failure of prohibition in the 1920's is the classic example. While this principle has less force in a military establishment than in civilian life, nevertheless in the activities of military organizations which are not directly related to combat, the principle has substantial force.

In the case of information security, while the need for it is accepted in the abstract, the need is not so keenly felt as in many other matters. It is not difficult for an infantryman to appreciate the need for the skillful use of ground cover when an enemy is shooting at him; but the intelligence agents of a potential enemy work quietly, and it is easy to forget their existence in the press of getting things done. We are aware that there are procedures throughout the Department designed to bring home the importance of information security by way of indoctrination and the like, and we commend these efforts. We think, however, that they are too largely confined to the lower echelons and that their effect has worn thin with those of higher rank.

Nor is the reasonableness of the security rules accepted as fully as it should be. On that score overclassification plays an important part. When much is classified that should not be classified at all, or is assigned an unduly high classification, respect for the system is diminished and the extra effort required to adhere faithfully to the security procedures seems unreasonable.

But the lack of a keen appreciation that security regulations are both necessary and reasonable is not the only cause for the existing lack of discipline in the field of security information. These are lacks on the positive side of discipline. Discipline however has a negative side - punishment. Even in this country punishment is recognized as an essential element of discipline. And we think disciplinary action has not been adequate in the field of security information, even after making due allowance for the difficulties generally encountered in identifying those responsible for violations.

VI. Recommendations on the Two Major Shortcomings.

With the foregoing considerations in mind, we recommend as follows:

A. Overclassification.

Recommendation No. 1. We recommend that a determined attack be made on overclassification. We think this should be spearheaded by the responsible heads within the Department of Defense, from the Secretary of Defense down, registering a keen interest in information security.

In any organization, particularly a military one, the example of the head of the organization has a potent influence on the whole organization. If he is interested in a particular subject, his immediate subordinates will be aware of it and will make sure that they are interested too. This interest will flow down the chain of command in a surprisingly short time until it permeates the entire organization.

There are many ways by which this keen interest may be evidenced. An important one is for the responsible head to make a point of personally checking the classification of documents coming across his desk, sending back with displeasure those which have been overclassified. This should be supplemented by evidencing a personal interest in the contents of a paragraph dealing with information security, which we recommend below be included in each program. An examination of the detailed recommendations which follow will suggest other ways of registering interest.

Our second recommendation sets forth other steps which we think should be taken to reduce overclassification. We have received a great many suggestions and recommend the following as having merit:

Recommendation No. 2a. Extend the use of classification guides now existing in several technical fields to other areas, and supplement the regulations covering general classification by developing guidelines and listing typical examples for each category of classification.

Department of Defense Directive 5230.12 (attached as Tab D) is an admirable example of a technical classification guide, except that it could

well prescribe the appropriate category of classification. On general classification, it should prove helpful to list certain categories as requiring a high degree of protection, such as strategic plans, future programs, design details, detailed performance data, new developments, operational methods, deployment, information as to our own specific weaknesses, and sources of our information regarding a potential enemy.

Recommendation No. 2b. Carry down the line Recommendation No. 1 made with respect to top officials, that superiors throw back over-classified matter received from subordinates.

At one time there was a requirement for the superior to initial a stamped form indicating his approval of the classification assigned, but this became routine and we think it would again, and do not recommend its reinstatement.

Recommendation No. 2c. Cut down the number who are authorized to classify information as Top Secret and to receive copies of Top Secret papers.

Executive Order 10501 contemplates a more specific designation of those authorized to use this category than the regulations of the Services now provide. This should be corrected, and at the same time a real effort made to limit more severely the distribution of copies of Top Secret documents.

Recommendation No. 2d. Require that each program or order susceptible of such treatment contain a special paragraph dealing with information security.

This paragraph should prescribe the degree of classification for the various elements of the program, establishing if possible automatic declassification on a certain date or happening of a certain event, and should force a deliberate decision on the harmful effect on security of an early deadline.

Recommendation No. 2e. Make wholly clear that the classification system is not to be used to protect information not affecting the national

security, and specifically prohibit its use for administrative matters.

Recommendation No. 2f. Cease attempts to do the impossible and stop classifying information which cannot be held secret.

This includes information which cannot be withheld because it inevitably is known to too many people. It includes the physical appearance and general performance data of new weapons when they have become widely known. It also includes compiled data composed of unclassified items and information which is already public, where official confirmation would not be of substantial value to a potential enemy, even though it will require additional machinery to keep track of what information has been publicly revealed.

Recommendation No. 2g. Improve procedures for releasing information as to the existence and general nature of differences of opinion between the several Services to permit authorized representatives to express Service views without disparaging their sister Services, and without, of course, disclosing information which is classified for reasons other than differences in military concept between the Services.

This recommendation really falls under No. 2f above, but it is also related to "leaks" in that it would tend to reduce the pressure causing them, and it is of sufficient importance to justify a recommendation by itself. There is no doubt that the existence of the differences of opinion between the Services, and their general nature, is widely known. Any attempt to cover up their existence and general nature not only creates great pressure to "leak" but creates an undesirable and inaccurate impression in the public mind that the Secretary of Defense is trying to cover up grave issues which he cannot solve. That tends to shake the confidence of the public in our whole defense set-up. Some of the press argue vigorously that the present procedures permitting disclosure of the issues are inadequate, that here are issues of great national importance on which the rightness of the final decision cannot be demonstrated short of war, and for decisions to be wholeheartedly supported the public must be informed; they should not

be decided in secret by a small group, however high their rank. Public discussion, they say, will not embarrass the Secretary of Defense if he takes the position that the problems are difficult; that he will consider all views and reach a decision only after the most careful consideration and with the very best advice he can obtain. They argue that under such circumstances publicity will help him because he will then receive understanding support from the public. If this argument contemplates going further than the limited publicity recommended above, we think it goes too far. Decisions on military planning involve facts the disclosure of which would be most harmful to the security of the nation. It seems to us that those decisions must be left in the future, as they have in the past, to the military experts under supervision of the civilians made responsible by law, with proper Congressional participation. We therefore urge the improved procedures recommended above without passing on the merits of the foregoing argument, and on the simple ground that it is futile and harmful to try to hide the existence and general nature of Service differences. We should like to add that no one with whom we talked has advocated that once a decision is made, the Services be permitted to dispute those decisions in public.

Recommendation No. 2h. Avoid changing the scope of classified information to reflect temporary changes in emphasis in our foreign policy.

As noted above, this may not be overclassification in the strict sense but many of the press think it is and it creates serious confusion in the already difficult task of applying the criteria to determine classification all over the world.

Recommendation No. 2i. Establish within the Office of the Secretary of Defense (possibly within the office of the Administrative Secretary) an official who would be responsible for establishing, directing and monitoring an active declassification program both in the Office of the Secretary of Defense and the military departments.

This official should be divorced from the direct influence of both security and public information officials in order to bring an unbiased, dispassionate and realistic judgment to the field of declassification. He

should likewise be of sufficient experience and knowledge to exercise mature discretion in matters affecting national policy vis-a-vis national security. After appropriate study, it might prove desirable to establish similar offices with comparable stature and mission in the military departments. In coordination with each other, means might then be found for simplifying declassification procedures and for eliminating the necessity of laboriously clearing each declassification action with the originating office. Except where inappropriate, notification as to declassification action should also be reduced to a simple circularizing process, such as periodical bulletins, post-cards, etc. We have been advised that the Interdepartmental Committee on Internal Security is studying the government-wide problem of declassification, and that the Department of Defense is participating in the preparation of that Committee's report. In view of this pending study and of the complexity of the problem, we have not conducted a thorough examination of the total Department of Defense declassification problem. Nevertheless, we have penetrated the matter sufficiently to determine that while at first glance this particular problem presents an utter maze of complexities and frustrations, more effective steps should be taken toward finding a practical solution to the immediate situation. Therefore, it is in the sense of making a start on a seemingly insurmountable problem that we recommend consideration of establishing the official described above.

It should be noted that some of the measures proposed in the foregoing recommendations (particularly f) may be of some help to a potential enemy, but the chances are they would do no more than save him some time and effort. On balance we think there is more to be gained than lost in adopting the recommendations.

It is obvious that some of the foregoing recommendations will require the expenditure of money. For instance, i involving declassification, and f involving better machinery for keeping track of information which has already been officially released, will require more money. But we think that the comparatively modest additional expense required is well worth while.

The foregoing recommendations concerning classification do not purport to be exhaustive. They represent our selection from all those submitted to us. In their implementation it is probable that others

equally adapted to attaining the desired objectives will suggest themselves.

B. Deliberate Unauthorized Disclosure.

We think an important step in preventing deliberate unauthorized disclosure of classified information is to eliminate delay in instituting investigations.

The existing investigatory machinery within the Department of Defense consists primarily of the machinery of the three military departments. The Office of the Secretary of Defense does not have machinery designed to handle a full scale investigation. In appropriate cases the Department can and does call upon the Federal Bureau of Investigation; but the military departments carry the main load. While we are not equipped to make a detailed examination of the competence and impartiality of the machinery of the military departments it is our distinct impression that their investigators are fully competent and have a professional pride in their work which produces impartiality. We see no reason to create a new organization of investigators responsible directly to the Secretary of Defense.

We do think, however, that someone directly responsible to the Secretary of Defense should be charged with maintaining the closest contact with investigations, in order to make sure that they are promptly initiated and vigorously pursued, no matter where they lead, and that the information produced by investigators reaches the top levels for action, and that appropriate action is taken. We further think that, for the purpose of refuting any allegation of Service bias if for no other reason, provision should be made for the participation of more than one Service in important investigations.

We have already alluded to the difficulty frequently encountered in identifying the source of "leaks." We are not convinced that this difficulty is insurmountable, and we think some action can and should be taken to overcome it.

Accordingly we propose as our third recommendation the following actions:

Recommendation No. 3a. We recommend that the Secretary of Defense make one person of stature in his office responsible for seeing that investigations are initiated with utmost

promptness on the occurrence of a "leak," and are vigorously pursued.

At present the responsibility is divided between the Assistant Secretary of Defense (Manpower, Personnel and Reserve) and the General Counsel, with the Assistant Secretary of Defense (Legislative and Public Affairs) participating at least to the extent of identifying and weighing the seriousness of the "leak." Whether the responsibility should be centered in one of those, or in someone else, is a matter of organization on which we do not feel competent to recommend; but whoever is selected, procedures should be established providing for the appropriate participation of the other interested elements of the Secretary's office.

Recommendation No. 3b. We further recommend that the Secretary of each military department start the investigating machinery of his department going instantly upon the occurrence of an unauthorized disclosure and follow the progress of the investigation closely.

Recommendation No. 3c. In the case of a serious "leak," we recommend that the Secretary or military Chief of each military department convene a Court of Inquiry composed in each case of representatives of the three military departments.

Each of the three Courts should be charged with investigation within one of the military departments and its progress should be closely followed by the official in the Office of the Secretary of Defense described in 3a above.

Recommendation No. 3d. In case of a "leak" appearing in the press which involves the disclosure of information which obviously gravely damages the security of the nation, and where the source of the "leak" cannot be identified, we recommend that the author be summoned to testify in a grand jury investigation in order to discover the source of the "leak."

As to disciplinary action itself we have the following recommendations:

Recommendation No. 4a. When a member of the Department of Defense has been identified as the source of a "leak," stern disciplinary action should be taken, and taken with the utmost promptness.

It seems to us that in the past, disciplinary action has often been too lenient and too slow. We think that, however high the motives of the individual may seem to himself, he is guilty of a serious offense and should be dealt with accordingly.

Recommendation No. 4b. In cases where it is clear, from a "leak" or otherwise, that an individual has not accepted a decision reached by the Secretary of Defense or higher authority, we recommend that prompt and stern disciplinary action be taken, whatever the rank of the individual may be.

Recommendation No. 4c. Commanding officers should be held responsible for security derelictions within their commands.

Even where it has proved impossible to identify the source of a "leak," we do not think that all disciplinary action is necessarily defeated. Since the advent of organized military forces, dependent for their functioning on a chain of command, it has been inherent in the system to hold a commander accountable for derelictions or ineffectiveness in the discharge of his responsibilities. In war and peace, commanders of all ranks and positions have been relieved and frequently demoted for failures in various aspects of the art of command. Violations of security affecting the national security are as serious as many other derelictions of command and should be treated as such by administrative action of a disciplinary nature. This should apply through the whole hierarchy of command.

We think the recommendations contained in this Part VI of our report should result in substantial progress in overcoming the two major shortcomings of overclassification and unauthorized disclosures.

VII. Unauthorized Disclosures of Administrative Matters.

So far in this report our concern has been primarily with classified information and we have merely noted that certain administrative matters, such as the advice of staff members to their superiors, often do not affect the national security and that in such case they should be protected under Department of Defense Directive 5200.6 and not by the classification system.

The vast majority of our people, both military and civilian, are well indoctrinated in the need for preserving the integrity of information dealing with military operations, such as war plans, and to a lesser degree of information less obviously relating to the national security. However, in the case of administrative matters which do not involve national security, but which nevertheless should not be publicly disclosed, there is every indication that such matters do not share the same regard. The impression is wide-spread that papers that do not bear a classification stamp (even if stamped "FOR OFFICIAL USE ONLY" and regardless of their import) are fit subjects for disclosure and discussion both within and outside the Department, even though in view of the provisions of Department of Defense Directive 5200.6, that disclosure involves a breach of discipline as much as the disclosure of classified information. The reason for this may be that responsibility for the administration of this Directive has not been fixed. It has not been assigned to the various security offices and it is on the periphery of the responsibilities of the various administrative offices.

We therefore submit the following as our fifth recommendation:

Recommendation No. 5a. Responsibility for protecting administrative matters entitled to protection should be definitely fixed.

Our view is that it should be assigned to the various security offices, since the problem of protecting administrative matters is essentially no different than protecting classified information, even though the basis for the protection is different. Whether or not this is the proper administrative move, the main point is to fix responsibility somewhere.

Recommendation No. 5b. Department of Defense Directive 5200.6 should be amended to add to the information protected by paragraph III A 3 f information relating to the

advice on official matters which personnel of the Department of Defense exchange with each other; and paragraph III B should be amended to make the use of the stamp "FOR OFFICIAL USE ONLY" compulsory on all future documents entitled to protection under Directive 5200.6.

Recommendation No. 5c. A vigorous program of indoctrination should be initiated among all personnel to instill a regard for the safeguarding of administrative matters entitled to protection under Directive 5200.6.

Recommendation No. 5d. In serious cases of unauthorized disclosures of these administrative matters, investigations and disciplinary action similar to that recommended above in connection with "leaks" of classified information should be undertaken, with the same person in the Office of the Secretary of Defense being responsible for initiating and following up investigations.

VIII. Industry.

We think that industry does a satisfactory job in protecting classified information, except in one aspect. Indeed some companies do an outstanding job. The exception is that in their desire to build up prestige some companies give out damaging technical information in their annual reports to stockholders, in advertisements, at business conferences and to trade and technical journals. This is especially true in connection with the production of new weapons, and it applies both to prime and subcontractors. As a part of our sixth recommendation we therefore recommend:

Recommendation No. 6a. More effective efforts should be made to educate the officers of offending companies, followed if necessary by the withdrawal of clearance of offending individuals, plus in extreme cases diversion of future business.

We have received compelling evidence of the real harm caused by information published in trade and technical journals. In some cases the data disclosed approaches complete specifications and detailed performance data of new planes or weapons -- matters which are of the greatest help in enabling a potential enemy to attain superiority in that vital field by taking advantage of our progress or concentrating on counter measures. This information appears to be derived from visits to manufacturing plants and conversations with manufacturer's personnel.

Recommendation No. 6b. We recommend that the Department of Defense take vigorous measures to stop this type of "leak, " and suggest that strengthening amendments to the Industrial Security Manual designed to limit to unclassified information the information obtainable from contractors and subcontractors by representatives of trade and technical journals would be an effective method to accomplish the desired result.

IX. Congress.

We have not included as unauthorized disclosures in this report classified information given to Congress. While we believe damage to the national security can, and sometimes does, come from disclosure of classified information furnished Congress, Congress will not, and in our opinion should not, authorize the large appropriations necessary to support the national defense effort without adequate information. The problem of security is well understood by both Congress and the Department of Defense, and procedures are available which, if followed by both branches of the government with understanding and good will, should produce a reasonably satisfactory degree of information security. We urge both branches to continue their efforts to insure that this mutual understanding and good will exists at all times. In so doing we think that both branches should keep in mind that unfriendly nations can glean a great deal of valuable information from the published reports of proceedings before Congressional Committees. Granted that these Committees should have a great deal of information, it seems to us unnecessary and highly undesirable to publish to the world information of great help to a potential enemy.

Recommendation No. 7. Care should be exercised to see that the published reports of proceedings before Congressional Committees do not contain classified operational concepts or technical data concerning new weapons and installations.

X. The Press.

We have alluded to the press a number of times in this report. In so doing we mean not only the newspapers, but also the wire services, magazines, radio, television -- in short all non-technical news media. We think we have their point of view clearly in mind, insofar as such a diverse and individualistic group may be said to have a single point of view.

It is our conclusion that in spite of the keen competition in the collection of news, and in spite of the resulting tendency of some to underrate the aid disclosures can give a potential enemy, or the discomfort disclosures can give our allies, or the importance of interim security for information which will ultimately be released, nevertheless the press is fully as loyal to the nation as any other segment of our population. Indeed we have run across instances where information of high news value has been voluntarily withheld, only to have it "scooped" by someone less scrupulous. It is true that we have also run across instances where a member of the press has made it clear that he is disclosing the contents of a Top Secret document. We think that is a disservice to the United States which is wholly inexcusable, even after making due allowance for the existing tendency to overclassify.

It has been suggested to us that some form of voluntary censorship by the press could be organized if a proper approach were made to leaders of the press. After careful consideration we do not recommend it. We believe that the competitive element in news gathering is too strong for any such attempt to be successful. We think past experience proves that this may not be done short of censorship, and that should war come, whether a major or minor war, censorship will be readily accepted by the press.

It has been proposed to us that all information given to the press should flow through the Office of Public Information and that the present practice of permitting direct access by the press to members of the

Department of Defense should be discontinued. We do not favor this proposal; we think it is in the nature of a partial censorship. We do however believe that the Office of Public Information cannot effectively perform its proper function if it has not at least general information as to who has been interviewed by members of the press and if it is not available when requested to assist in such interviews.

We also believe that some members of the press do not fully appreciate the marked difference between ordinary peacetime and the present so-called "cold war." While we are confident that the press can be counted on not to publish information which they determine will significantly damage the security of the nation, we believe that in making their own determination some of them tend to ignore the difference between ordinary peace and today's international situation. In 1948 Dr. Vannevar Bush made an able presentation to the press of the problem of information security on technical matters as it existed at that time. We think that presentation is equally applicable today, and attach a copy as Tab E.

Accordingly as our eighth recommendation we recommend:

Recommendation No. 8a. All interviews by the press with members of the Department of Defense in the Washington area should be arranged through the Office of Public Information and, if so requested by the person to be interviewed, a representative of that Office should attend the interview.

Recommendation No. 8b. A forceful statement outlining the differences between ordinary peace and the present situation from the point of view of information security should be prepared and given wide distribution to the press.

Recommendation No. 8c. When a request by the press for the release of information is denied on the ground that the information is classified, the press should be told why it is classified. The bald statement that it is classified often creates in their minds the feeling that the refusal is wholly arbitrary. Of course in some cases the full

background is too sensitive to be disclosed. Nevertheless we think more can be done along these lines.

XI. Concentration of Implementation.

It is impossible for us to draw geographical lines delineating those areas in which the problems we have discussed are the most acute, and those areas in which they are less acute. Nevertheless we are convinced that the Washington area contains by far the largest number of problems and that they are by far the most acute. It is there that the future of the Services is decided, and there that the mass of classified papers is generated, and there that the number of officials with over-all knowledge is the greatest.

We therefore submit our ninth recommendation:

Recommendation No. 9. Implementation
of the recommendations of this report
should be concentrated on the Washington
area.

Not only should this simplify implementation, but if the situation in Washington can be improved, we believe improvement in the field would follow almost automatically.

XII. General Conclusions.

Our examination leads us to conclude that there is no conscious attempt within the Department of Defense to withhold information which under the principles set forth at the beginning of this report the public should have; that the classification system is sound in concept and, while not operating satisfactorily in some respects, it has been and is essential to the security of the nation; and that further efforts should be made to cure the defects in its operation.

XIII. Summary of Recommendations.

For convenience there follows a summary of our recommendations.

Recommendation No. 1. Make a determined attack on over-classification, spearheaded by the responsible heads within the Department of Defense, from the Secretary of Defense down. (page 10)

Recommendation No. 2a. Supply guides to overcome the generality of classification criteria. (page 10)

Recommendation No. 2b. Broaden Recommendation No. 1 by requiring that all superiors reject overclassified material received from subordinates. (page 11)

Recommendation No. 2c. Cut down the number who are authorized to classify information as Top Secret and to receive copies of Top Secret papers. (page 11)

Recommendation No. 2d. Require that each program or order susceptible of such treatment contain a special paragraph dealing with information security. (page 11)

Recommendation No. 2e. Make wholly clear that the classification system is not to be used to protect information not affecting the national security. (page 11)

Recommendation No. 2f. Cease attempts to classify information which cannot be held secret. (page 12)

Recommendation No. 2g. Improve procedures for releasing information as to the existence and general nature of differences of opinion between the several Services to permit authorized representatives to express Service views, without disparaging their sister Services, and without, of course, disclosing information which is classified for reasons other than differences in military concept between the Services. (page 12)

Recommendation No. 2h. Avoid changing scope of classified information to reflect temporary changes in emphasis in our foreign policy. (page 13)

Recommendation No. 2i. Establish within the Office of the Secretary of Defense an official who will be responsible for establishing and monitoring an active declassification program. (page 13)

Recommendation No. 3a. Designate one official in the Office of the Secretary of Defense as responsible for seeing that investigations of "leaks" are initiated with utmost promptness on their occurrence and are vigorously pursued. (page 15)

Recommendation No. 3b. Within each military department start investigating machinery going instantly upon occurrence of an unauthorized disclosure. (page 16)

Recommendation No. 3c. Convene Courts of Inquiry of tri-service composition in case of a serious "leak." (page 16)

Recommendation No. 3d. In case of a "leak" appearing in the press which obviously gravely damages the security of the nation, and where the source of the "leak" cannot be identified, summons the author to testify in a grand jury investigation in order to discover the source. (page 16)

Recommendation No. 4a. Take prompt and stern disciplinary action when the source of a "leak" is identified. (page 17)

Recommendation No. 4b. Take prompt and stern disciplinary action when an individual has not accepted a decision reached by the Secretary of Defense or higher authority. (page 17)

Recommendation No. 4c. Hold Commanders responsible for security derelictions within their commands. (page 17)

Recommendation No. 5a. Fix responsibility for protecting administrative matters. (page 18)

Recommendation No. 5b. Amend Department of Defense Directive 5200.6 to include protection for information relating to advice on official matters and compel use of "FOR OFFICIAL USE ONLY" stamp on all future documents entitled to protection under that Directive. (page 18)

Recommendation No. 5c. Initiate a program of indoctrination among all personnel of the Department of Defense to instill a proper regard for safeguarding of all information protected by Department of Defense Directive 5200.6. (page 19)

Recommendation No. 5d. Take appropriate and prompt investigative and disciplinary action in cases of unauthorized disclosure of information on these administrative matters. (page 19)

Recommendation No. 6a. Take steps to develop a better understanding in certain parts of industry of the hazards to national security resulting from disclosure of certain technical classified information. (page 19)

Recommendation No. 6b. Take vigorous steps to stop leaks to trade and technical journals. (page 20)

Recommendation No. 7. Exercise care in the publishing of reports of proceedings before Congressional Committees to eliminate sensitive technical data and classified operational concepts. (page 21)

Recommendation No. 8a. Arrange interviews with Department of Defense members through the Office of Public Information, with a representative sitting in if requested. (page 22)

Recommendation No. 8b. Release a forceful statement to the press outlining the differences between ordinary peace and the present situation from the point of view of information security. (page 22)

Recommendation No. 8c. Give reasons for classification whenever possible when requests for information are denied. (page 22)

Recommendation No. 9. Concentrate implementation of these recommendations on the Washington area. (page 23)

Respectfully submitted:

Charles A. Coolidge

Charles A. Coolidge, Chairman

William M. Fechteler

Admiral William M. Fechteler, USN (Ret.)

John E. Hull

General John E. Hull, USA (Ret.)

Gerald C. Thomas

General Gerald C. Thomas, USMC (Ret.)

Idwal H. Edwards

Lieutenant General Idwal H. Edwards, USAF (Ret.)

November 8, 1956.

THE SECRETARY OF DEFENSE

WASHINGTON

August 13, 1956

Dear Mr. Coolidge:

As you are aware, I am seriously concerned over the unauthorized disclosure of classified military information. I am, therefore, forming a committee to study the problem and suggest methods and procedures to eliminate this threat to the national security.

I appreciate your willingness to be chairman of the committee. I am asking a senior retired officer from each Military Service to serve with you. I will appreciate it if you and your committee will undertake an examination of the following matters affecting national security:

1. A review of present laws, Executive Orders, Department of Defense regulations and directives pertaining to the classification of information and the safeguarding of classified information, to evaluate the adequacy and effectiveness of such documents.
2. An examination of the organizations and procedures followed within the Department of Defense designed to implement the above cited documents, to evaluate the adequacy and effectiveness of such organizations and procedures.
3. An examination of the means available to the Department of Defense to fix responsibility for the unauthorized disclosure of classified information, and to determine the adequacy and effectiveness of such means in preventing future unauthorized disclosures of such information.
4. An examination of the organizations and procedures in the Department of Defense designed to prevent the inadvertent disclosure of classified information in any manner.

I realize that the above problem areas are complex, and I want your committee to have adequate opportunity to go into them thoroughly.

In view of the extreme seriousness of the matter, however, I would appreciate an interim report as soon as possible.

Sincerely,

C. E. Wilson

Honorable Charles A. Coolidge
Department of Defense
Washington 25, D. C.

EXECUTIVE ORDER No. 10501

NOVEMBER 5, 1953

SAFEGUARDING OFFICIAL INFORMATION IN THE INTERESTS OF THE DEFENSE OF THE UNITED STATES

WHEREAS it is essential that the citizens of the United States be informed concerning the activities of their government; and

WHEREAS the interests of national defense require the preservation of the ability of the United States to protect and defend itself against all hostile or destructive action by covert or overt means, including espionage as well as military action; and

WHEREAS it is essential that certain official information affecting the national defense be protected uniformly against unauthorized disclosure:

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes, and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

Section 1. CLASSIFICATION CATEGORIES

Official information which requires protection in the interests of national defense shall be limited to three categories of classification, which in descending order of importance shall carry one of the following designations: Top Secret, Secret, or Confidential. No other designation shall be used to classify defense information, including military information, as requiring protection in the interests of national defense, except as expressly provided by statute. These categories are defined as follows:

(a) Top Secret: Except as may be expressly provided by statute, the use of the classification Top Secret shall be authorized, by appropriate authority, only for defense information or material which requires the highest degree of protection. The Top Secret classification shall be applied only to that information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation such as leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.

(b) Secret: Except as may be expressly provided by statute, the use of the classification Secret shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could result in serious damage to the Nation, such as by jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important intelligence operations.

(c) Confidential: Except as may be expressly provided by statute, the use of the classification Confidential shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.

Section 2. LIMITATION OF AUTHORITY TO CLASSIFY

The authority to classify defense information or material under this order shall be limited in the departments and agencies of the executive branch as hereinafter specified. Departments and agencies subject to the specified limitations shall be designated by the President:

(a) In those departments and agencies having no direct responsibility for national defense there shall be no authority for original classification of information or material under this order.

(b) In those departments and agencies having partial but not primary responsibility for matters pertaining to national defense the authority for original classification of information or material under this order shall be exercised only by the head of the department or agency, without delegation.

(c) In those departments and agencies not affected by the provisions of subsection (a) and (b), above, the authority for original classification of information or material under this order shall be exercised only by responsible officers or employees, who shall be specifically designated for this purpose. Heads of such departments and agencies shall limit the delegation of authority to classify as severely as is consistent with the orderly and expeditious transaction of Government business.

Section 3. CLASSIFICATION

Persons designated to have authority for original classification of information or material which requires protection in the interests of national defense under this order shall be held responsible for its proper classification in accordance with the definitions of the three categories in section 1, hereof. Unnecessary classification and over-classification shall be scrupulously avoided. The following special rules shall be observed in classification of defense information or material:

(a) Documents in General: Documents shall be classified according to their own content and not necessarily according to their relationship to other documents. References to classified material which do not reveal classified defense information shall not be classified.

(b) Physically Connected Documents: The classification of a file or group of physically connected documents shall be at least as high as that of the most highly classified document therein. Documents separated from the file or group shall be handled in accordance with their individual defense classification.

(c) Multiple Classification: A document, product, or substance shall bear a classification at least as high as that of its highest classified component. The document, product, or substance shall bear only one over-all classification, notwithstanding that pages, paragraphs, sections, or components thereof bear different classifications.

(d) Transmittal Letters: A letter transmitting defense information shall be classified at least as high as its highest classified enclosure.

(e) Information Originated by a Foreign Government or Organization: Defense information of a classified nature furnished to the United States by a foreign government or international organization shall be assigned a classification which will assure a degree of protection equivalent to or greater than that required by the government or international organization which furnished the information.

Section 4. DECLASSIFICATION, DOWNGRADING, OR UPGRADING

Heads of departments or agencies originating classified material shall designate persons to be responsible for continuing review of such classified material for the purpose of declassifying or downgrading it whenever national defense considerations permit, and for receiving requests for such review from all sources. Formal procedures shall be established to provide specific means for prompt review of classified material and its declassification or downgrading in order to preserve the effectiveness and integrity of the classification system and to eliminate accumulation of classified material which no longer requires protection in the defense interest. The following special rules shall be observed with respect to changes of classification of defense material:

(a) Automatic Changes: To the fullest extent practicable, the classifying authority shall indicate on the material (except telegrams) at the time of original classification that after a specified event or date, or upon removal of classified enclosures, the material will be downgraded or declassified.

(b) Non-Automatic Changes: The persons designated to receive requests for review of classified material may downgrade or declassify such material when circumstances no longer warrant its retention in its original classification provided the consent of the appropriate classifying authority has been obtained. The downgrading or declassification of extracts from or paraphrases of classified documents shall also require the consent of the appropriate classifying authority unless the agency making such extracts knows positively that they warrant a classification lower than that of the document from which extracted, or that they are not classified.

(c) Material Officially Transferred: In the case of material transferred by or pursuant to statute or Executive order from one department or agency to another for the latter's use and as part of its official files or property, as distinguished from transfers merely for purposes of storage, the receiving department or agency shall be deemed to be the classifying authority for all purposes under this order, including declassification and downgrading.

(d) Material Not Officially Transferred: When any department or agency has in its possession any classified material which has become five years old, and it appears (1) that such material originated in an agency which has since become defunct and whose files and other property have not been officially transferred to another department or agency within the meaning of subsection (c), above, or (2) that it is impossible for the possessing department or agency to identify the originating agency, and (3) a review of the material indicates that it should be downgraded or declassified, the said possessing department or agency shall have power to declassify or downgrade such material. If it appears probable that another department or agency may have a substantial interest in whether the classification of any particular information should be maintained, the possessing department or agency shall not exercise the power conferred upon it by this subsection, except with the consent of the other department or agency, until thirty days after it has notified such other department or agency of the nature of the material and of its intention to declassify or downgrade the same. During such thirty-day period the other department or agency may, if it so desires, express its objections to declassifying or downgrading the particular material, but the power to make the ultimate decision shall reside in the possessing department or agency.

(e) Classified Telegrams: Such telegrams shall not be referred to, extracted from, paraphrased, downgraded, declassified, or disseminated, except in accordance with special regulations issued by the head of the originating department or agency. Classified telegrams transmitted over cryptographic systems shall be handled in accordance with the regulations of the transmitting department or agency.

(f) Downgrading: If the recipient of classified material believes that it has been classified too highly, he may make a request to the reviewing official who may downgrade or declassify the material after obtaining the consent of the appropriate classifying authority.

(g) Upgrading: If the recipient of unclassified material believes that it should be classified, or if the recipient of classified material believes that its classification is not sufficiently protective, it shall be safeguarded in accordance with the classification deemed appropriate and a request made to the reviewing official, who may classify the material or upgrade the classification after obtaining the consent of the appropriate classifying authority.

(h) Notification of Change in Classification: The reviewing official taking action to declassify, downgrade, or upgrade classified material shall notify all addressees to whom the material was originally transmitted.

Section 5. MARKING OF CLASSIFIED MATERIAL

After a determination of the proper defense classification to be assigned has been made in accordance with the provisions of this order, the classified material shall be marked as follows:

(a) Bound Documents: The assigned defense classification on bound documents, such as books or pamphlets, the pages of which are permanently and securely fastened together, shall be conspicuously marked or stamped on the outside of the front cover, on the title page, on the first page, on the back page and on the outside of the back cover. In each case the markings shall be applied to the top and bottom of the page or cover.

(b) Unbound Documents: The assigned defense classification on unbound documents, such as letters, memoranda, reports, telegrams, and other similar documents, the pages of which are not permanently and securely fastened together, shall be conspicuously marked or stamped at the top and bottom of each page, in such manner that the marking will be clearly visible when the pages are clipped or stapled together.

(c) Charts, Maps, and Drawings: Classified charts, maps, and drawings shall carry the defense classification marking under the legend, title block, or scale in such manner that it will be reproduced on all copies made therefrom. Such classification shall also be marked at the top and bottom in each instance.

(d) Photographs, Films and Recordings: Classified photographs, films, and recordings, and their containers, shall be conspicuously and appropriately marked with the assigned defense classification.

(e) Products or Substances: The assigned defense classification shall be conspicuously marked on classified products or substances, if possible, and on their containers, if possible, or, if the article or container cannot be marked, written notification of such classification shall be furnished to recipients of such products or substances.

(f) Reproductions: All copies of reproductions of classified material shall be appropriately marked or stamped in the same manner as the original thereof.

(g) Unclassified Material: Normally, unclassified material shall not be marked or stamped Unclassified unless it is essential to convey to a recipient of such material that it has been examined specifically with a view to imposing a defense classification and has been determined not to require such classification.

(h) Change or Removal of Classification: Whenever classified material is declassified, downgraded, or upgraded, the material shall be marked or stamped in a prominent place to reflect the change in classification, the authority for the action, the date of action, and the identity of the person or unit taking the action. In addition, the old classification marking shall be cancelled and the new classification (if any) substituted therefor. Automatic change in classification shall be indicated by the appropriate classifying authority through marking or stamping in a prominent place to reflect information specified in subsection 4 (a) hereof.

(i) Material Furnished Persons not in the Executive Branch of the Government: When classified material affecting the national defense is furnished authorized persons, in or out of Federal service, other than those in the executive branch, the following notation, in addition to the assigned classification marking, shall whenever practicable be placed on the material, on its container, or on the written notification of its assigned classification:

"This material contains information affecting the national defense of the United States within the meaning of the espionage laws, Title 18, U.S.C., Secs. 793 and 794, the transmission or revelation of which in any manner to an unauthorized person is prohibited by law."

Use of alternative marking concerning "Restricted Data" as defined by the Atomic Energy Act is authorized when appropriate.

Section 6. CUSTODY AND SAFEKEEPING

The possession or use of classified defense information or material shall be limited to locations where facilities for secure storage or protection thereof are available by means of which unauthorized persons are prevented from gaining access thereto. Whenever such information or material is not under the personal supervision of its custodian, whether during or outside of working hours, the following physical or mechanical means shall be taken to protect it:

(a) Storage of Top Secret Material: Top Secret defense material shall be protected in storage by the most secure facilities possible. Normally it will be stored in a safe or a safe-type steel file container having a three-position, dial-type, combination lock, and being of such weight, size, construction, or installation as to minimize the possibility of surreptitious entry, physical theft, damage by fire, or tampering. The head of a department or agency may approve other storage facilities for this material which offer comparable or better protection, such as an alarmed area, a vault, a secure vault-type room, or an area under close surveillance of an armed guard.

(b) Secret and Confidential Material: These categories of defense material may be stored in a manner authorized for Top Secret material, or in metal file cabinets equipped with steel lockbar and an approved three combination dial-type padlock from which the manufacturer's identification numbers have been obliterated, or in comparably secure facilities approved by the head of the department or agency.

(c) Other Classified Material: Heads of departments and agencies shall prescribe such protective facilities as may be necessary in their departments or agencies for material originating under statutory provisions requiring protection of certain information.

(d) Changes of Lock Combinations: Combinations on locks of safekeeping equipment shall be changed, only by persons having appropriate security clearance, whenever such equipment is placed in use after procurement from the manufacturer or other sources, whenever a person knowing the combination is transferred from the office to which the equipment is assigned, or

whenever the combination has been subjected to compromise, and at least once every year. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest category of classified defense material authorized for storage in the safekeeping equipment concerned.

(e) Custodian's Responsibilities: Custodians of classified defense material shall be responsible for providing the best possible protection and accountability for such material at all times and particularly for securely locking classified material in approved safekeeping equipment whenever it is not in use or under direct supervision of authorized employees. Custodians shall follow procedures which insure that unauthorized persons do not gain access to classified defense information or material by sight or sound, and classified information shall not be discussed with or in the presence of unauthorized persons.

(f) Telephone Conversations: Defense information classified in the three categories under the provisions of this order shall not be revealed in telephone conversations, except as may be authorized under section 8 hereof with respect to the transmission of Secret and Confidential material over certain military communications circuits.

(g) Loss or Subjection to Compromise: Any person in the executive branch who has knowledge of the loss or possible subjection to compromise of classified defense information shall promptly report the circumstances to a designated official of his agency, and the latter shall take appropriate action forthwith, including advice to the originating department or agency.

Section 7. ACCOUNTABILITY AND DISSEMINATION

Knowledge or possession of classified defense information shall be permitted only to persons whose official duties require such access in the interest of promoting national defense and only if they have been determined to be trustworthy. Proper control of dissemination of classified defense information shall be maintained at all times, including good accountability records of classified defense information documents, and severe limitation on the number of such documents originated as well as the number of copies thereof reproduced. The number of copies of classified defense information documents shall be kept to a minimum to decrease the risk of compromise of the information contained in such documents and the financial burden on the Government in protecting such documents. The following special rules shall be observed in connection with accountability for and dissemination of defense information or material:

(a) Accountability Procedures: Heads of departments and agencies shall prescribe such accountability procedures as are necessary to control effectively the dissemination of classified defense information, with particularly severe control on material classified Top Secret under this order. Top Secret Control Officers shall be designated, as required, to receive, maintain accountability registers of, and dispatch Top Secret material.

(b) Dissemination Outside the Executive Branch: Classified defense information shall not be disseminated outside the executive branch except under conditions and through channels authorized by the head of the disseminating department or agency, even though the person or agency to which dissemination of such information is proposed to be made may have been solely or partly responsible for its production.

(c) Information Originating in Another Department or Agency: Except as otherwise provided by section 102 of the National Security Act of July 26, 1947, c. 343, 61 Stat. 498, as amended, 50 U.S.C. sec. 403, classified defense information originating in another department or agency shall not be disseminated

outside the receiving department or agency without the consent of the originating department or agency. Documents and material containing defense information which are classified Top Secret or Secret shall not be reproduced without the consent of the originating department or agency.

Section 8. TRANSMISSION

For transmission outside of a department or agency, classified defense material of the three categories originated under the provisions of this order shall be prepared and transmitted as follows:

(a) Preparation for Transmission: Such material shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and address. The outer cover shall be sealed and addressed with no indication of the classification of its contents. A receipt form shall be attached to or enclosed in the inner cover, except that Confidential material shall require a receipt only if the sender deems it necessary. The receipt form shall identify the addressor, addressee, and the document, but shall contain no classified information. It shall be signed by the proper recipient and returned to the sender.

(b) Transmitting Top Secret Material: The transmission of Top Secret material shall be effected preferably by direct contact of officials concerned, or, alternatively, by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system especially created for that purpose, or by electric means in encrypted form; or in the case of information transmitted by the Federal Bureau of Investigation, such means of transmission may be used as are currently approved by the Director, Federal Bureau of Investigation, unless express reservation to the contrary is made in exceptional cases by the originating agency.

(c) Transmitting Secret Material: Secret material shall be transmitted within the continental United States by one of the means established for Top Secret material, by an authorized courier, by United States registered mail, or by protected commercial express, air or surface. Secret material may be transmitted outside the continental limits of the United States by one of the means established for Top Secret material, by commanders or masters of vessels of United States registry, or by United States Post Office registered mail through Army, Navy, or Air Force postal facilities, provided that the material does not at any time pass out of United States Government control and does not pass through a foreign postal system. Secret material may, however, be transmitted between United States Government and/or Canadian Government installations in continental United States, Canada, and Alaska by United States and Canadian registered mail with registered mail receipt. In an emergency, Secret material may also be transmitted over military communications circuits in accordance with regulations promulgated for such purpose by the Secretary of Defense.

(d) Transmitting Confidential Material: Confidential defense material shall be transmitted within the United States by one of the means established for higher classifications, by registered mail, or by express or freight under such specific conditions as may be prescribed by the head of the department or agency concerned. Outside the continental United States, Confidential defense material shall be transmitted in the same manner as authorized for higher classifications.

(e) Within an Agency: Preparation of classified defense material for transmission, and transmission of it, within a department or agency shall be governed by regulations, issued by the head of the department or agency, insuring a degree of security equivalent to that outlined above for transmission outside a department or agency.

Section 9. DISPOSAL AND DESTRUCTION

Documentary record material made or received by a department or agency in connection with transaction of public business and preserved as evidence of the organization, functions, policies, operations, decisions, procedures or other activities of any department or agency of the Government, or because of the informational value of the data contained therein, may be destroyed only in accordance with the act of July 7, 1943, c. 192, 57 Stat. 380, as amended, 44 U.S.C. 366-380. Non-record classified material, consisting of extra copies and duplicates including shorthand notes, preliminary drafts, used carbon paper, and other material of similar temporary nature, may be destroyed, under procedures established by the head of the department or agency which meet the following requirements, as soon as it has served its purpose:

(a) Methods of Destruction: Classified defense material shall be destroyed by burning in the presence of an appropriate official or by other methods authorized by the head of an agency provided the resulting destruction is equally complete.

(b) Records of Destruction: Appropriate accountability records maintained in the department or agency shall reflect the destruction of classified defense material.

Section 10. ORIENTATION AND INSPECTION

To promote the basic purposes of this order, heads of those departments and agencies originating or handling classified defense information shall designate experienced persons to coordinate and supervise the activities applicable to their departments or agencies under this order. Persons so designated shall maintain active training and orientation programs for employees concerned with classified defense information to impress each such employee with his individual responsibility for exercising vigilance and care in complying with the provisions of this order. Such persons shall be authorized on behalf of the heads of the departments and agencies to establish adequate and active inspection programs to the end that the provisions of this order are administered effectively.

Section 11. INTERPRETATION OF REGULATIONS BY THE ATTORNEY GENERAL

The Attorney General, upon request of the head of a department or agency or his duly designated representative, shall personally or through authorized representatives of the Department of Justice render an interpretation of these regulations in connection with any problems arising out of their administration.

Section 12. STATUTORY REQUIREMENTS

Nothing in this order shall be construed to authorize the dissemination, handling or transmission of classified information contrary to the provisions of any statute.

Section 13. "RESTRICTED DATA" AS DEFINED IN THE ATOMIC ENERGY ACT

Nothing in this order shall supersede any requirements made by or under the Atomic Energy Act of August 1, 1946, as amended. "Restricted Data" as defined by the said act shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1946, as amended, and the regulations of the Atomic Energy Commission.

Section 14. COMBAT OPERATIONS

The provisions of this order with regard to dissemination, transmission, or safekeeping of classified defense information or material may be so modified in

connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe.

Section 15. EXCEPTIONAL CASES

When, in an exceptional case, a person or agency not authorized to classify defense information originates information which is believed to require classification, such person or agency shall protect that information in the manner prescribed by this order for that category of classified defense information into which it is believed to fall, and shall transmit the information forthwith, under appropriate safeguards, to the department, agency, or person having both the authority to classify information and a direct official interest in the information (preferably, that department, agency, or person to which the information would be transmitted in the ordinary course of business), with a request that such department, agency, or person classify the information.

Section 16. REVIEW TO INSURE THAT INFORMATION IS NOT IMPROPERLY WITHHELD HEREUNDER

The President shall designate a member of his staff who shall receive, consider, and take action upon, suggestions or complaints from non-Governmental sources relating to the operation of this order.

Section 17. REVIEW TO INSURE SAFEGUARDING OF CLASSIFIED DEFENSE INFORMATION

The National Security Council shall conduct a continuing review of the implementation of this order to insure that classified defense information is properly safeguarded, in conformity herewith.

Section 18. REVIEW WITHIN DEPARTMENTS AND AGENCIES

The head of each department and agency shall designate a member or members of his staff who shall conduct a continuing review of the implementation of this order within the department or agency concerned to insure that no information is withheld hereunder which the people of the United States have a right to know, and to insure that classified defense information is properly safeguarded in conformity herewith.

Section 19. REVOCATION OF EXECUTIVE ORDER NO. 10290

Executive Order No. 10290 of September 24, 1951 is revoked as of the effective date of this order.

Section 20. EFFECTIVE DATE

This order shall become effective on December 15, 1953.

DWIGHT D. EISENHOWER

THE WHITE HOUSE,

November 5, 1953.



1 June 1954
NUMBER 5200.6

Department of Defense Directive

SUBJECT Policy Governing the Custody, Use and Preservation of Department of Defense Official Information Not Within the Purview of Executive Order No. 10501

References: (a) Revised Statutes, Sec. 161 (5 U.S.C. 22)
(b) Sec. 3 of the Act of June 11, 1946 (60 Stat. 238; 5 U.S.C. 1002)
(c) Sec. 1 of the Act of June 25, 1948 (62 Stat. 791; 18 U.S.C. 1905)

I. PURPOSE

- A. Pursuant to statutory requirements, to assure the proper custody, preservation and use of official information which requires protection in the public interest, but which is not within the purview of Executive Order No. 10501.
- B. To authorize the use of the term "For Official Use Only" within the Department of Defense for identifying this type of official information.
- C. To avoid arbitrary and unreasonable withholding of such information, but to assure that official information not within the purview of Executive Order No. 10501 is released only by authorities who are competent to determine whether release is prejudicial to the public interest.

II. BACKGROUND

- A. Records and files of an executive agency of the Government, in the absence of specific statutory restriction, are generally subject to the right of inspection by persons having a legitimate interest in such records and files. The principal exception to the general rule concerning the right of inspection provides that the use of official records may be subjected to appropriate restrictions when the head of the agency deems such restrictions are required in the public interest.

- B. The authority for imposing restrictions on the use of public records is derived primarily from reference (a) which permits the head of a department to issue regulations, not inconsistent with law, governing the custody, preservation and use of the records of his department. Reference (b) provides generally that, except for (1) any function of the United States requiring secrecy in the public interest or (2) any matter relating solely to the internal management of an agency, the records of an agency of the Government shall be made available to persons properly and directly concerned, except information "held confidential for good cause found." Reference (c) provides for penalties for disclosure of official information which would be in violation of law.

III. POLICY

- A. 1. All documents, material, technical information or any other information relating to the operations and activities of the Department of Defense are considered official information.
2. That official information which requires protection in the interests of national defense is so protected under the provisions of Executive Order 10501, dated 5 November 1953, "Safeguarding Official Information in the Interests of the Defense of the United States," and implementing Department of Defense Directives Number 5200.1, dated 19 November 1953, and Number 5200.3, dated 21 December 1953.
3. Certain other official information, not within the purview of Executive Order 10501, requires protection in accordance with statutory requirements or in the public interest. Such information includes, but is not limited to, the following:
- a. Records and information which pertain to individuals such as personnel records, medical records, and investigative reports, documents, and proceedings.
 - b. Information as to the identity of confidential informants and information furnished by them in confidence.
 - c. Information received in confidence from private individuals, firms, or organizations in connection with bids, proposals, "trade secrets", and reports of a financial, technical, or scientific nature.
 - d. Information which is, or may reasonably be expected to be, connected with any pending or anticipated litigation before Federal and state courts or regulatory bodies.

1 June 54
5200.6

- e. Advance information on proposed plans to procure, lease or otherwise acquire or dispose of materials, real estate, facilities, or functions, which would provide undue or discriminatory advantage to private or personal interests.
 - f. Preliminary documents relating to proposed plans or policy development when premature disclosure would adversely affect morale, efficiency or discipline.
 - g. Examination questions and answers to be used in training courses or in the determination of qualifications of candidates for employment, entrance to duty and advancement or promotion.
- B. In order to assure uniformity within the Department of Defense for identifying information such as listed in Section III A 3 above, the term "For Official Use Only" is authorized. The use of the term is optional and the conditions under which it will be used shall be prescribed by the Secretaries of the Military Departments and the Assistant Secretary of Defense (Manpower and Personnel). Information such as described in Section III A 3 above will be afforded protection as required, regardless of whether or not the information is identified by the term "For Official Use Only."
- C. Release of official information such as described in Section III A 3 above will be authorized only upon a determination by a responsible official that the request for such information is based upon a legitimate interest, and that its release will not be prejudicial to the public interest or contrary to law. The arbitrary and unreasonable withholding of such information will be avoided. In this connection, the identifying term "For Official Use Only" will be removed promptly when there is no longer a specific justification for protecting such information.

IV. ACTION

The Secretaries of the Military Departments and the Assistant Secretary of Defense (Manpower and Personnel) will insure that adequate regulations have been, or are, issued to implement the policy stated herein with regard to the protection and authorized release of the official records and information of their respective agencies.

V. IMPLEMENTATION

It is requested that copies of implementing instructions be furnished this office when issued.

VI. EFFECTIVE DATE

This Directive is effective immediately.



Acting Secretary of Defense



March 27, 1956
NUMBER 5230.12

(Public Information Security Guidance No. 19)

Department of Defense Directive

SUBJECT Release to the Public of Information on Guided Missiles,
Military Aircraft, Associated Powerplants, Components
and/or Accessories

Reference: (a) Department of Defense Directive 5230.9, dated
March 29, 1955, subject: "Clearance of Department
of Defense Public Information"

Enclosures: (1) Appendix - Release Schedule for Military Aircraft
(2) Appendix - Release Schedule for Military Engines
(3) Appendix - Release Schedule for Guided Missiles

I. PURPOSE

This directive provides public information security guidance governing the review of all information concerning guided missiles, military aircraft, associated powerplants, components and/or accessories prior to its release to the public. It is applicable to:

- A. All agencies and offices of the Department of Defense.
- B. All contractors or subcontractors who receive Department of Defense contracts, letters of intent, or supplemental agreements for development or production.

II. POLICIES GUIDING THE RELEASE OF PUBLIC INFORMATION

- A. The premature release to the public of information pertaining to guided missiles, military aircraft, associated powerplants, components and/or accessories may constitute a grave threat to national security. It is necessary to safeguard this information and establish uniform action within the Department of Defense consistent with the principles of reference (a).

- B. The provisions of this directive do not abrogate the authority and responsibility of the Secretaries of the Military Departments regarding the security classification and declassification of projects under their cognizance.
- C. Authority is hereby delegated to the Director, Office of Security Review, Office of the Assistant Secretary of Defense (Legislative and Public Affairs) for final clearance for release to the public of information described herein.
- D. The placement of military aircraft, guided missiles, associated powerplants, components and/or accessories into the appropriate phases of development and production (see attached appendices) will remain the responsibility of the Secretaries of the Military Departments.
- E. It is recognized that instances will arise which, because of their sensitivity or other overriding factor, cannot be readily resolved within the guidance contained herein. Each such case will be considered by the Office of the Secretary of Defense and resolved on its own merit. Any decision in such a case will not be considered as establishing a precedent.

III. PROCEDURES AND APPLICATION

- A. The appendices are guides only to the releasability of information to the public and will not be considered as authority for automatic release. Information previously authorized for public release by the Office of the Secretary of Defense may be released or re-released to the public without further approval. However, prior unofficial publication of the types of information described herein does not constitute authority for official release. If the information pertains to classified contracts or projects, the contractor shall be guided by Paragraph 6N of Industrial Security Manual for Safeguarding Classified Information.
- B. Organizations and personnel to whom this directive is applicable will submit proposed public releases in accordance with existing directive issuances.
- C. The attached aircraft appendices will not apply to rotary wing, training, liaison, search and rescue, glider-type, or research aircraft. Proposed public release of information on these aircraft will be considered individually when submitted for review.

Mar 27, 56
5230.12

- D. Information pertaining to military aircraft, guided missiles, powerplants, components and/or accessories which have been cancelled, discontinued, completed or are beyond the phases outlined in the attached appendices will be considered for public release on an individual basis.

IV. IMPLEMENTATION

The Secretaries of the Military Departments will issue instructions to implement this directive. Implementing directives should re-emphasize the necessity for subcontractors to coordinate with prime contractors on matters pertaining to release of information on subjects covered by this directive.

V. EFFECTIVE DATE

This Directive is effective as of this date. In accordance with Section VII, DOD Directive 5025.1, dated January 31, 1956, three copies of the proposed implementation of the Directive on Release of Information will be forwarded, within 30 days, to the Assistant Secretary of Defense (L&PA), for review and approval prior to their issuance by the Military Departments.



Secretary of Defense

Mar 27, 56 (Encl 1)
5230.12

APPENDIX

RELEASE SCHEDULE FOR MILITARY AIRCRAFT

Phases of Development and Production: *

1. Preliminary design and studies and Phase I contracts through mockup.
2. Phase II contracts from mockup until factory roll-out of first production aircraft.
3. Factory roll-out of first production aircraft until combat or training units receive first production aircraft.
4. After operational or training units are receiving production aircraft.

* Production aircraft refers to the first aircraft of an unbroken series produced for inventory in accordance with an established production schedule.

Items of Information	Category I Aircraft of New Design				Category II Improvements of Existing Aircraft			
	1	2	3	4	1	2	3	4
a. Model designation & Mfg. and Powerplant Model & Mfg.	NR	R	R	R	NR	R	R	R
b. General engineering principles & aerodynamic design information.	NR	NR	NR	NR	NR	NR	NR	NR
c. Physical characteristics which include external photographs, drawings, dimensions, models and launchers.	NR	NR	R	R	NR	NR	R	R
d. Performance in Generalities.	NR	NR	R	R	NR	NR	R	R
e. Exact Performance and Characteristics data.	NR	NR	NR	NR	NR	NR	NR	NR
f. Internal Photographs and Drawings.	NR	NR	NR	NR*	NR	NR	NR	NR*

Mar 27, 56 (Encl 1)
5230.12

APPENDIX

RELEASE SCHEDULE FOR MILITARY AIRCRAFT (Cont'd)

Items of Information	Category I Aircraft of New Design				Category II Improvements of Existing Aircraft			
	1	2	3	4	1	2	3	4
g. Armament details which can not be ascertained from external inspection.	NR	NR	NR	NR	NR	NR	NR	NR
* Certain internal photographs, drawings, and dimensions that do not reveal significant details may be considered for release.								

Mar 27, 56 (Encl 3)
5230.12

APPENDIX

RELEASE SCHEDULE FOR GUIDED MISSILES

Phases of Development and Production: *

1. Preliminary design and studies and Phase I contracts through mockup.
2. Phase II contracts from mockup through Research and Development Models and R&D operation, includes prototype and technical evaluation.
3. From the start of production through service acceptance of the first production model and through equipping and using units, including logistics activities in support thereof.

* Production guided missile refers to the first guided missile of an unbroken series produced for inventory in accordance with an established production schedule.

Items of Information	Category I Missiles of New Design			Category II Model Improvements of Existing Missiles		
	1	2	3	1	2	3
a. Model designation & Mfg.	NR	NR	R	NR	NR	R
b. Production schedules and capabilities, number of missiles per contract, unit cost per missile, delivery rate.	NR	NR	NR	NR	NR	NR
c. General engineering principles and aerodynamics design information.	NR	NR	NR	NR	NR	R
d. Performance in generalities.	NR	NR	R	NR	NR	R
e. Exact performance.	NR	NR	NR	NR	NR	NR
f. External physical characteristics of missiles and launchers which include photos, drawings, dimensions and miniature models.	NR	NR	R	NR	NR	R

APPENDIX

RELEASE SCHEDULE FOR GUIDED MISSILES (Cont'd)

Items of Information	Category I Missiles of New Design			Category II Model Improvements of Existing Missiles		
	1	2	3	1	2	3
g. Internal photos, drawings and dimensions.	NR	NR	NR*	NR	NR	NR*
h. Power plant **Mfg & type.	NR	NR	R	NR	NR	R
i. Power plant model.	NR	NR	R	NR	NR	R
j. Armament details, including fuzeing.	NR	NR	NR	NR	NR	NR
k. Specific details of control, guidance, launching and propulsion.	NR	NR	NR	NR	NR	NR
l. Design studies.	NR	NR	NR	NR	NR	NR
m. General propulsion and launching system information.	NR	NR	R	NR	NR	R

* Certain internal photographs, drawings and dimensions that do not reveal significant details may be considered for release.

** The term power plant includes any method of motivation such as air breathing, solid or liquid propellant, engine motor, etc.

OFFICE OF THE SECRETARY OF DEFENSE
Washington, D.C.

HOLD FOR RELEASE
FRIDAY, APRIL 16, 1948, 2:45 PM, EST

APRIL 16, 1948
NO. 51-48

Remarks of Vannevar Bush, Chairman, Research
and Development Board, and President, Carnegie
Institution of Washington, Before American Society
of Newspaper Editors, Statler Hotel, Washington, D.C.

As the second World War reached its end, Mr. Churchill, commenting on the possible future action of Russia, declared that "It is a riddle wrapped up in a mystery inside of an enigma." Much the same characterization applies to the problem of security of technical military information in a great democratic nation such as ours in times of international tension such as these. I do not by any means profess to have an answer to this riddle. But the problem as a whole is one to which I have given a lot of hard thinking, and I can at least put some results of that before you.

We are all fully aware that aggression is still loose in the world, and that the peril of outright armed aggression and consequently of sudden full-scale war is as real today as it was ten years ago. We know, too, that the nature of warfare has undergone a sweeping and fundamental change in the past decade, so that today the well-being of nations, the potentialities of the United Nations as a stabilizing force, and the hope of a final and lasting peace depend as never before on continuing and successful development of the advanced weapons, the advanced techniques, which science and technology have made available to the military art. We know full as well that unless we safeguard our own advances in these fields, we may expect to fight a possible future war with weapons as good as obsolete because the enemy knows both what they are and how to counter them. That is, we know that if we are careless, if we are gullible, we not only lose the staggering power of surprise, but indeed give that power over to the enemy in double terms.

There is the essence of the problem. The quick, obvious and easy answer of course is, "Tell nothing to anyone." But easy answers don't make sense generally, and this one is no exception. There are other factors of very great importance to the problem.

Principal among these is our realization that the bulwark of the democratic process is an informed public opinion. The whole history

of this country is a demonstration that the free exchange of ideas and complete accessibility of information are vital to the national welfare. In the narrower and more specialized field of fundamental science, as in public affairs, freedom of information, active and alert interchange of ideas, are, we know, equally imperative for growth and advancement. It is no mere matter of custom and tradition -- it is a practical fact of experience -- that sound administration of a representative republic depends on the education of the electorate through the ample supply of information through publication, and that vigorous and dynamic scientific activity similarly depends upon the crossfertilization of trained minds through uninhibited and generous interchange of ideas.

The riddle wrapped up in a mystery inside of an enigma, then, is the problem of reconciling the preservation of the values inherent in the practice of full and free dissemination of fact with the common-sense requirement that we do not put into a potential enemy's hands information which will help him to kill our young men, devastate our cities, and overthrow our nation. The problem is that of distinguishing between information which rightly and properly belongs to every man and information which for the safety and security of every man must be protected. In terms of the military research and development with which we are immediately concerned, the problem is that of defining in the process from research through development to procurement the point where the law of diminishing returns begins to operate on publication. That is the point where the possible peril to the total national safety because of the publication of a piece of information is greater than any possible gain from such publication.

In evaluating facts to determine this point, we have constantly to bear in mind that the art of the spy is to put a half-dozen seemingly innocent facts together and from them to draw conclusions which may be fatal to our interests. You will recall a newspaper's account of the Battle of Midway, which included the order of battle of the Japanese fleet. That information added nothing to the value of the story to any ordinary reader, but made it damningly plain to any enemy agent who saw it that the United States was in possession of the Japanese code. By some dispensation, our enemies did not make use of that fact to institute new codes. Had they done so, and had they as a result been able to conceal their further plans from us, the welfare of the United States would indeed have been jeopardized. The fact of our possession of their code was secret information and should have been so regarded by all of us. The fact that it was not is a reminder that all too easily, through over-confidence, bad judgment, or occasionally and worst of all,

out and out irresponsibility, this matter of security can be misjudged as a mere battle of wits between publicists on the one hand and military men on the other. This is a dangerous and damnable misconception. The battle of wits is between the United States and a potential future enemy, and there can be no question, to my mind, of where that fact means the allegiance of all of us belongs, or of the requirements which it imposes on us.

In that battle of wits, we do well to pay full heed to certain of the long proved principles of actual warfare. Among those of the very highest importance is that of defense in depth, and this applies very decidedly in the matter of protecting information essential to security. The field commander who safeguarded vital bases only by garrisoning them, whose supply depots were protected only by a corporal's guard, with no outposts, would not last twenty-four hours in modern warfare. So it is in the research and development whose purpose is to provide advanced and powerful weapons to our armed forces. Here, if we either do not seek out the critical point of which I have spoken, or ignore it when it is determined, but go ahead with the development and wait to impose secrecy until the finished weapon has been produced, we are being exactly as misguided and stupid. It is not enough thus to protect merely the last vital boundary, to protect a vital base merely by garrisoning it. There must be first, second, third -- sometimes even more -- lines of defense around vital developments as well as around vital bases. We can compete in the open with any totalitarian power and give them cards and spades as far as fundamental science -- the foundation on which development rests -- is concerned. It would be difficult for us so to compete if we followed the totalitarian model and regimented ourselves in this regard. But in the applications which grow through development out of fundamental science, it is a different matter. The critical point may well be reached far earlier in the process than we are accustomed to think, and for the safety of the republic we must be alert to it and ready at once to erect the defenses of protection and security which it demands.

Sometimes in discussions of this problem of determining the delicate point where common sense and the common good demand that information become protected, you will hear it argued that no secret can be kept very long anyhow. This argument flies in the face of the facts. For example, consider the technique of pulse detection of submarines -- Asdic as it used to be called. The United States put a lot of effort into that technique, and developed it to a high point of effectiveness over a considerable period of years. There was no leak such as that in the Japanese code affair. The Nazis therefore went in complete ignorance

of the entire development, and as a result for a long time lost U boats. The truth of the matter is that this is the primary reason why their submarine campaign did not at once get off to a heavy start in the early part of the war. As we all know, when it finally did go into high gear, it dealt us losses that could well have been decisive but for the fact that our shipbuilding effort by then had had opportunity to go into still higher gear. It took time for that to happen, and the secrecy which had surrounded Asdic -- the secret which had been kept and well kept -- gave the United States and its Allies the time demanded.

Another and greater secret, extending over a long period and involving a large number of people, is involved in the development of the atomic bomb. Do not misunderstand me here as suggesting that there is a so-called secret of the bomb -- a single set of two or three facts that could be put down on a slip of paper and would enable anyone who wanted to to go ahead and build bombs. What I am referring to is a different sort of thing -- the fact that we had under way in this country in the midst of a terrible war the development of a new, titanically powerful weapon and were diverting scarce and vital materials and manpower to completing it. Knowledge of this would unquestionably have affected the war plans, the strategy, the choice of weapons and techniques, of all our enemies. A leak here might well have had fatal consequences. There was no leak.

Those are demonstrations that the thing can be done. They show that the critical point can be determined, however it may vary as between different kinds of projects, and that once it has been determined, Americans can cooperate in maintaining the kind of control essential to the common defense. Today, we have few real secrets, but they are ones which we must protect, and to protect them under the democratic way, we must cooperate freely and honestly with one another. I am sure this can be done, because it is being done today and because the information in question is reasonably easy of definition. Absolute secrecy about the very existence of experimental projects may be undesirable as well as impossible. But on the contrary, there may be very good reason for protecting the fact that we are engaged in experimentation of a particular sort, that is, for not letting a potential enemy know a particular fashion in which we are marshaling part of our strength. Technical details, of course, must be guarded all along the way, but we cannot dismiss the problem with that. Of very great importance indeed to the national welfare is information about the success or nonsuccess, the efficiency, the effectiveness, of results. It is absurd to tell a possible enemy that a certain weapon development is successful, for thus we specify to him the counter effort which he

should take. It is equally absurd to tell him that some other undertaking has failed, for thus we advise him not to try it and so we help him to make better preparations against us.

The National Military Establishment is taking definite steps for the better handling of its aspect of the whole problem -- which means really safeguarding the responsible publicist against pitfalls into which he might stumble because of irresponsibility on the part of others, as much as it means insuring that the heavy assignment of the Establishment to assure the defense of the nation is fully and properly met.

I am sure that as we go on, joint effort can be counted on when critical points are reached and protective action is needed. The freedom of the press is involved here, yes, and rightly so. The press of the democratic world today is the only press which has freedom, freedom to publish, and, be it remembered, freedom not to publish when in its considered judgment -- in the considered judgment of sincere and responsible men, the greater good is served by following common-sense requirements to protect information that might be of aid and comfort to the enemy.

THE ARMY LIBRARY

WASHINGTON, D. C.