Depts 6

DCI/IC 75-3237

Cross Ref:
[redacted]
Security (3)

7 November 1975

MEMORANDUM FOR: [redacted] 25X1

SUBJECT: Secrecy Study

25X1 [redacted]

1. This memorandum will confirm the details of our recent conversation relating to the study you have been requested to undertake on behalf of the DCI.

2. In short, we are looking for a reasonably brief philosophical statement on secrecy and compartmentation and the strengths and weaknesses related to these matters. We ask that the paper focus on the various elements of intelligence activities and describe in pro and con fashion the requirements for secrecy and compartmentation in (a) research and development of intelligence collection systems, (b) collection and processing activities and (c) analysis and production.

3. There four primary objectives to be considered in the preparation of the paper.

(1) We need to make the intelligence product simple for the right consumers to obtain and receive.

(2) We need to knock down compartmentation when it lacks justification and stands in the way of solid management procedures.

(3) We need to identify those areas of intelligence activities which must be cloaked with strong secrecy arrangements so that we can aid and assist in the development of ~~imposed~~ Those secrecy arrangements. And,

(4) We need to identify those areas of intelligence activities which can be opened up more widely than they are now.

4. We need a preliminary (if not final) paper from you on these matters prior to Friday, 21 November.

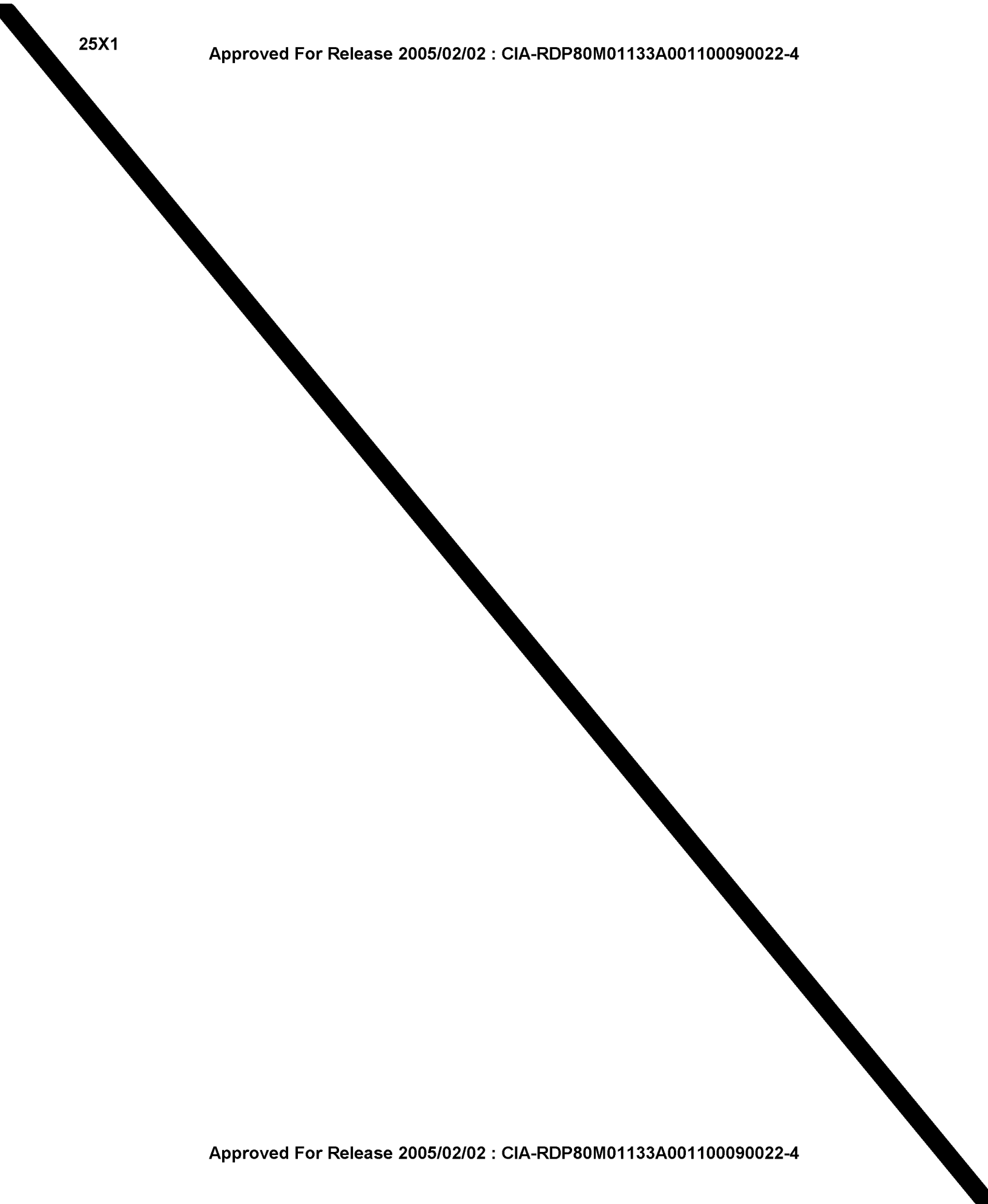
5. In the course of your study, you should feel free to consult with various members of the IC Staff, particularly Major General [redacted] CIA authorities to be consulted include the DDI who has strong personal views on these matters, and the General Counsel who is actively involved with the Justice Department in sketching out the details of new secrecy legislation. The precise action officers in the Office of the General Counsel are [redacted] and [redacted]

6. You should also consult with intelligence authorities outside of Langley, including DIA and perhaps NSA. Two USIB Committee Chairmen with direct interests in all this are [redacted] of COMIREX and [redacted] of SIGINT. Feel free to deal with them as well.

7. We know that we have given you a very tight and perhaps unrealistic deadline, but we simply must be able to address this problem with a preliminary paper and we have tasked you as one who is admirably equipped to look across the range of intelligence activities to help us get this job done well. We will help you in any way we can. Onward and upward!

[redacted]
E. H. Knoche
AD/DCI/IC

cc: General Counsel
DDI
C/COMIREX
C/SIGINT
C/CS/ICS



Approved For Release 2005/02/02 : CIA-RDP80M01133A001100090022-4

THE DIRECTOR OF CENTRAL INTELLIGENCE

WASHINGTON, D. C. 20505

Admiral George W. Anderson, Jr., USN (Ret.)
Chairman, President's Foreign
Intelligence Advisory Board
The White House
Washington, D. C. 20500

Dear Admiral:

I am writing now concerning heightened anxiety in the community and in my own mind over leaks to the press of sensitive intelligence data. I want to share with you and the Board my present appreciation of the problem and to seek your advice and recommendations.

As you well know, unauthorized public disclosures of intelligence information have occurred frequently in recent years. A more important consideration, however, is that press revelations have come increasingly to include explicit and generally accurate details about the methods we use to obtain and exploit sensitive information. In the past year we have witnessed a further upswing in the number and severity of damaging intelligence leaks--a situation I can only describe as a virtual hemorrhaging of the security control system. And it seems clear that journalists are not just being briefed orally: they are now being given direct access to highly classified documents.

Recently I had my staff take a fresh look at the problem to see if there were not some as yet untried way--within the means at my disposal--to halt and reverse this trend. Although I did this with a sense of having been through the exercise many times before, it was still essential to try again, not only because of the damage individual leaks can cause to our long-term capabilities, but because the present situation also generates widespread discouragement and frustration--even cynicism--within the ranks of the intelligence community itself. This has the potential for lowering security discipline even more.

In the past, expressions of serious concern over intelligence leaks have been voiced by successive Presidents and their department heads following a particularly grave leak or a series of damaging leaks. My predecessors and I have responded largely by trying to improve document and personnel security practices, issuing guidelines to Government departments on procedures for sanitizing the intelligence to be used by administration officials for public purposes, and carrying out investigations of the more flagrant and damaging leaks. These are all necessary steps, but clearly they have been insufficient, and simply repeating them will--in my view--prove no more effective now than in the past.

To tackle this problem constructively, I believe we must be quite frank. We have, I believe, focused so intently on the conditions that make intelligence leaks possible that we have slighted consideration of the climate of opinion in and out of Government that actually encourages them.

The widespread public dissemination of classified intelligence information does not represent a direct breakdown of the elaborate system of classification, document controls, personnel security checks, indoctrination practices, and application of the "need-to-know" principle which we use to minimize the risks of exposing sensitive data to the many persons who must work on and use them. The overwhelming number of such disclosures come not from the rank and file of analysts and drafters who were privy to the materials within the intelligence community. Rather, most represent deliberate disclosures by senior or relatively senior officials with an unquestionable "need to know"--most of them outside the intelligence community--who evidently believe that the public benefits of disclosing the information far outweigh the damage or risks involved.

Many disclosures identifiably represent a calculated "official" judgment at departmental level that previously classified material--say, on ICBM deployments--could be properly declassified and released. While other disclosures are usually less easy to pinpoint as to source, most of them appear designed to promote the programs, policies, or interests of particular elements within the Government--or to rebut those of others--as part of the continuing process in which national security policies are hammered out. Relatively few can be readily construed as the disclosures of a disgruntled or venal underling.

Most of the "official" disclosures noted above, and quite a few of the others, have probably involved no serious threat to intelligence sources and methods. A good deal of the intelligence we collect, notably in the area of overhead reconnaissance, is less sensitive than it once was. What is increasingly disregarded, however, is that there remain many sensitive areas of information and analysis, often identifiable as such only by intelligence specialists, where disclosure could be highly detrimental. Unfortunately, however, there is no established Government-wide procedure for determining who can declassify intelligence information and for assuring that it is properly sanitized before release, and there is a marked reluctance within the responsible Government departments to pursue investigations of potentially damaging disclosures that point toward relatively senior levels of officials. Meanwhile, the increasing frequency of disclosures of classified intelligence information--whether "official" or not--encourages the growth of a permissive atmosphere in which it seems that almost anything goes.

I see the press as largely an instrument in this process--not a direct cause of it. While there <u>are</u> examples of what I consider gratuitous and irresponsible exposure of sensitive data on the part of individual journalists, most of these persons see themselves as conforming to a widespread and generally accepted standard. Much of what they report has been made available to them by presumably responsible officials who clearly intended to have the information made public. And in the present atmosphere of disclosures, small wonder that many of the more energetic reporters feel that any information they can dig out is fair game.

In sum, I believe our basic problem is with an increasingly prevalent state of mind among many senior officials in the Executive Branch, among members of the press, and among many in the Congress. This involves a line of reasoning containing one or more of the following elements:

> The democratic process requires informed open debate, and if the price of that is an occasional risk to intelligence, it must be paid.

The intelligence community has been overprotective and unnecessarily secretive about sources and methods everyone knows it employs. Despite frequent alarms about the alleged damage caused by past disclosures, the US still has a highly effective system for collecting intelligence information. The problem, if any, is rather with how effectively it uses the material.

The "leakage" issue is at least partially a red herring, because every administration so far has selectively released intelligence information to its own advantage. There are complaints about "leaks" only when information which doesn't support the official view gets out.

That line of reasoning cannot lightly be dismissed: there is in fact much truth in it. The price of a free society must be paid if we are to retain the democratic process. The intelligence community probably has been overinclined to classify everything as a matter of course, and often overly shrill in claiming irreparable damage to its sources and methods when leaks have occurred. And there is some validity to the argument that the Government has at times appeared to follow a double standard in evaluating damage of intelligence disclosures and placing blame according to who makes them and whose policies they support.

Unfortunately, when the issue is posed in these terms the wrong dichotomy is emphasized. The proper question is not the public need to know versus the parochial interests of the intelligence services and the administration for self-protection. The issue is rather between the short-term and long-term interests of us all. In other words, a sound and defensible balance is needed between the contemporary domestic imperatives of an open society and the preservation of an ability in the future to detect dangers to that society that originate from abroad.

There are somewhat parallel dilemmas in other areas of Government which I have often referred to. For example, our military forces must be responsive to civilian control, but the public does not demand that detailed war plans be published. Our judicial system must meet the public's standards of justice, but

grand jury proceedings are not conducted in the open. It is even necessary for the Congress to conduct some of its business in executive session, while remaining accountable to the voters for the legislation it passes. What we no longer can count on is a general public understanding and acceptance of the need for similar trade-offs between openness and confidentiality in the field of foreign intelligence.

To deal with the problem of protecting vital sources and methods against unwarranted disclosure, there is a clear need to consider significant departures from the limited approaches that have been taken in the past. As I see it, there are several areas that call for careful and simultaneous attention:

Continued efforts within the intelligence community are needed to limit the opportunity for inadvertent or intended (but unauthorized) disclosures of classified information when the disclosures are made by persons in the intelligence services, and to facilitate successful investigation and application of penalties. A number of activities are under way within the USIB arena to study this problem and to make such changes as are necessary in the classification and compartmentation system and in controlling the dissemination of sensitive data.

There is also a need to develop more effective controls and sanctions relating to disclosures of foreign intelligence information by officials outside the intelligence services of Government departments. No adequate procedures or common standards exist for determining accountability for press disclosures or for guiding the preparation of authorized texts for public disclosures and for reporting them. This would require action by USIB in concert with several other departments of Government.

Ways need to be devised to discourage and if necessary penalize unauthorized disclosures by advocates of particular programs or policies within the Government and by contractors with access to intelligence data. The availability of judicial sanctions would be helpful in this regard--and I have proposed legislation to that end--but a greater degree of organizational

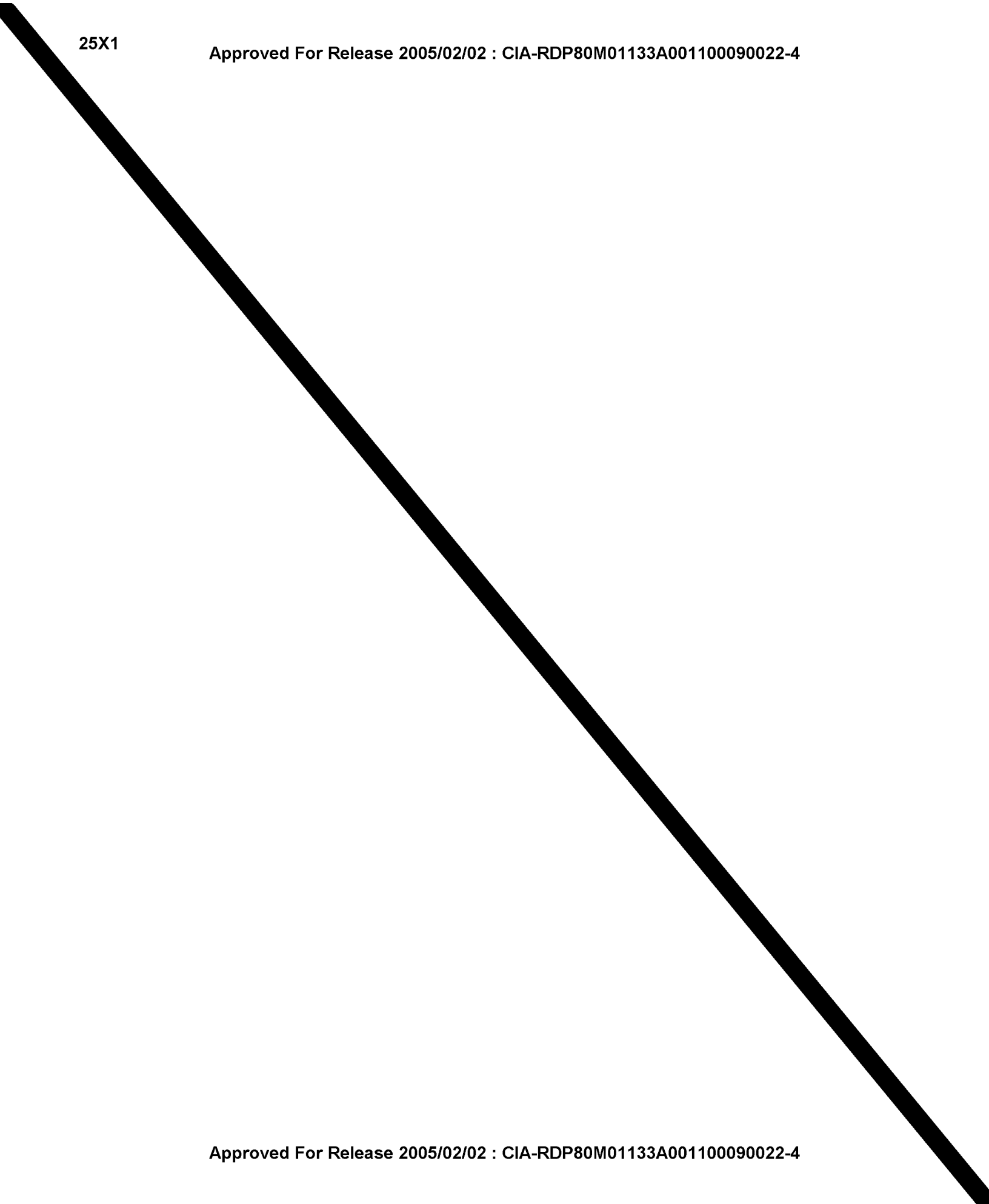
and ultimately self-imposed discipline by senior officials within Government is equally essential. This is probably the most difficult of all objectives to achieve. It lies almost wholly outside the intelligence community's ability to do more than seek to persuade, and it involves the delicate question of how each administration wishes to deal with adversary procedures within its own ranks. Its achievement would clearly require a significant change in attitude not only by the officials directly involved but ultimately by key elements in the Congress and the press and the public with whom they must deal. But I feel certain that the lack of such discipline has come to be a central weakness in our foreign intelligence security control system, and I would be derelict in not forthrightly saying so.

Finally, the intelligence community needs itself to re-examine its traditional classification standards and practices, with a view to being more forthcoming in making public those intelligence findings and materials whose disclosure would not create security problems or diplomatic difficulties or otherwise damage the national interest. Only if we are seen to be reasonable in such matters can we expect full acceptance of our demands for continued protection of data which remains sensitive. In this, a more careful distinction must be made among what I have termed good secrets, bad secrets, and non-secrets. I am taking some initiatives in this area but will wish to obtain the views of others--including the PFIAB--as well.

The situation we face is serious--and getting worse. It is almost overwhelming in its complexity and resistance to solution. The attitudinal factors which encourage disclosures are the dominant elements of my concern right now, because they feed and nourish the trend. And yet there is little I alone can do on that central problem. I have outlined some areas that need attention, and request your early consideration of them and your thoughts on how to proceed.

Sincerely,

W. E. Colby



Approved For Release 2005/02/02 : CIA-RDP80M01133A001100090022-4

SECRET

Executive Registry
75-3950

DCI/IC-75-0682
13 August 1975

MEMORANDUM FOR: Deputy to the DCI for the IC

SUBJECT : "Secrecy" Paper

1. Attached is a proposed approach to the "secrecy" problem assigned to you by the DCI following his discussion with the PFIAB on 7 August.

2. This is a rough first cut at an approach, and as the text indicates, it will need to be fleshed out in numerous places, probably by use of a task force. No one else has read this draft, so it does not reflect any "consensus."

25X1

3. In [redacted] view, during the discussion at the PFIAB meeting, the DCI seemed to favor an incremental approach to the problem, while several PFIAB members came out in favor of drastic change in the classification/compartment systems.

4. What I have sought to do is outline the approach, fill in part of the text, and included samplings of the ideas which I suggest that you discuss with the DCI to ascertain whether this is the kind of a paper he had in mind.

25X1

[redacted]
Major General, USAF (Ret.)
Chief, Coordination Staff, ICS

Attachment:
as stated

SECRET

25X1

THE APPLICATION OF SECURITY CLASSIFICATIONS AND COMPARTMENTATION IN INTELLIGENCE ACTIVITIES

PROBLEM

To assess the continued validity of the existing system of classification (as provided by E.O. 11652) and the compartmentation systems utilized by the U.S. Intelligence Community in view of the changing political and social U.S. attitudes toward secrecy in government, and to recommend such changes as the Director of Central Intelligence could sponsor.

BACKGROUND

1. This paper responds to a request made by the PFIAB at its 7 August 1975 meeting that the DCI address this problem at the next PFIAB meeting in October. PFIAB concerns relate to the recent spate of disclosures of sensitive intelligence information--as indicative that the current classification/compartmentation system is not working.

2. PFIAB expressions of a need for a new look at the classification/compartmentation picture relate to a widespread concern with "secrecy in government" reflected in numerous recent publications.*

FOUNDATION OF THE PRESENT SYSTEM: E.O. 11652

3. The opening three paragraphs of E.O. 11652, "Classification and Declassification of National Security Information and Material," dated 8 March 1972, present the philosophy of the existing system:

---

* In addition to magazine articles, newspaper columns and statements by Senators and Congressmen, three books which illustrate the kinds of criticisms being publicly expressed are:

Government Secrecy, Hearings before the Subcommittee on Intergovernmental Relations of the Committee on Government Operations, United States Senate, 93rd Congress, 2nd Session, on S.1520, S.1726, S.2451, S.2738, S.3393, and S.3399, May 22, 23, 29, 30, 31 and June 10, 1974 (908 pg.)

Secrecy and Foreign Policy, Edited by Thomas M. Franck and Edward Weisband, Oxford University Press, 1974 (453 pg.)

None of Your Business: Government Secrecy in America, Edited by Norman Dorsen and Stephen Gillers, Penguin Books, 1975

"The interests of the United States and its citizens are best served by making information regarding the affairs of the Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in current public information policies of the Executive Branch.

"Within the Federal Government there is some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our allies. To protect against actions hostile to the United States, of both an overt and covert nature, it is essential that such official information and material be given only limited dissemination.

"This official information or material, referred to as classified information or material in this order, is expressly exempted from public disclosure by Section 552(b)(1) of Title 5, United States Code. Wrongful disclosure of such information or material is recognized in the Federal Criminal Code as providing a basis for prosecution."

4. Definitions of security classification categories in E.O. 11652 are as follows:

Top Secret: "national security information or material which requires the highest degree of protection. The test for assigning "Top Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security."

(Among the examples the E.O. cites are "the compromise of complex cryptologic or communications intelligence systems; the revelation of sensitive intelligence operations...")

Secret: "national security information or material which requires a substantial degree of protection. The test for assigning "Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security."

(Among the examples the E.O. cites are "revelation of significant intelligence operations...")

Confidential: "national security information or material which requires protection. The test for assigning "Confidential" classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security."

5. "National Security" in all of the foregoing definitions is used in the collective sense of "the national defense or foreign relations of the United States."

6. The special compartmentation systems which organizations of the Intelligence Community have used as tools to protect particularly important or particularly sensitive information by controlling its dissemination and access are based on two sources of authority:

a. The provision of the National Security Act of 1947 which charges the Director of Central Intelligence with the responsibility for protecting intelligence sources and methods (which is also reflected in NSCID No. 1), and

b. Section 9 of E.O. 11652 which provides:

"Special Departmental Arrangements. The originating Department or other appropriate authority may impose, in conformity with the provisions of this order, special requirements with respect to access, distribution and protection of classified information and material, including those which presently relate to communications intelligence, intelligence sources and methods and cryptography."

DISCUSSION

7. Problems with the Security Classification System

a. While problems of security classification undoubtedly apply to various kinds of national security information or material other than those with which the Intelligence Community is concerned, this paper deals only with those which relate to intelligence and which, in some instances, are peculiar to intelligence--such as the protection of sensitive sources and methods.

b. Critics of classification, as used by intelligence organizations, cite the following:

(1) There are no objective standards to guide the classifiers and personal judgment plays too large a role. Overclassification tends to be the almost inevitable result.

(2) The system is not enforceable, as evidenced by numerous "unauthorized disclosures," a continuing inability to identify the sources of leaks, and a failure or inability to impose sanctions even if the source of the leak is identified.

(FLESH OUT WITH MORE CRITICISMS)

c. Supporters of the existing classification system emphasize:

(1) Despite its shortcomings, the present system imposes a sense of discipline, both on members of the Intelligence Community and on the recipients of the information.

(FLESH OUT WITH MORE DEFENSES)

8. Problems with the Compartmentation Systems

a. Critics of the existing systems of compartmentation cite that:

(1) Compartmentation is excessively used, with the result that often times those who require the information cannot have access.

(2) The unauthorized disclosure of even highly compartmented information demonstrates that rigidly applied "need to know" criteria does not prevent exposure of data the Intelligence Community considers particularly sensitive.

(FLESH OUT THE CRITICISMS)

b. Supporters of the use of compartments to restrict dissemination and access to sensitive information argue:

(1) Protection of truly sensitive sources and methods--and the resultant information--is of such importance that it justifies the effort even though experience has shown this is no guarantee against exposure.

(2) Proper application of the "need to know" criteria can ensure that those who require the information will have access to it.

(FLESH OUT THE SUPPORTING ARGUMENTS)

9. Factors Considered in Developing Alternative Approaches

a. The requirement to protect sensitive intelligence sources and methods is both real and imperative--the problem is to assure that the classification/compartmentalization process is applied only to that which really needs to be, and truly must be, protected.

b. The cloak of classification developed over the past 30 years, however justified it may have been, needs adjustment to the realities of the mid-1970's world--but adjustment with which the Intelligence Community can function effectively. The "that's classified" admonition now carries less weight and is accorded less support than has been the case during the developmental period of the U.S. Intelligence Community. Questions as to "why" or "for what reason" need to be squarely faced.

c. Considerations of "need to know" must be addressed in terms of a deliberate balance between the requirements of sophisticated users of the intelligence product and careful examination of what intelligence sources and methods truly need protection.

d. The public's "right to know" has spokesmen who today are more persuasive in many instances than those who would defend a pervasive intelligence classification and compartmentalization structure.

e. The present system of top secret-secret-confidential classifications is deeply ingrained in not only the Intelligence Community, but in the government as a whole as well, and any attempt to "tinker" with existing definitions probably would be unproductive.

f. There is need, however, for more definitive criteria for the application of classification categories. Present guidance allows too much leeway and depends more than it should on judgment factors which vary from one classifier to another. The factor of human judgment cannot be eliminated, but the uncertainty factor could be narrowed by guidance which is quite specific in nature.

g. "National security" as now defined in E.O. 11652 is not necessarily the only basis for the classification of official information. "National welfare" as influenced by intelligence on foreign energy developments, foreign resource use, changes in the world physical environment, etc. may also provide a basis for application of security classifications.

h. Whatever system of classification is applied by the Intelligence Community to its finished products must be one which the users of intelligence recognize as being useful, necessary and logical.

i. Nothing short of a basic overhaul of the compartmentation system, with its multiple use of codewords, is likely to satisfy the critics of the present system among the recipients of intelligence products.

j. Some statutory means of applying criminal sanctions to persons who are responsible for unauthorized disclosure of classified information would probably enhance the disciplinary effect of both classification and compartmentation systems.

(FLESH OUT WITH MORE FACTORS)

10. Action options

a. The classification/compartmentation problems now confronting the Intelligence Community can be addressed in terms of action options which are either incremental or major in scope. The following options are grouped accordingly. The basic tenet is that the Community is not in a position to "stand fast" on past and present procedures and practices. It must, in one way or another, reflect the changing U.S. concepts

of "national interest" and "national security" or risk statutory or other reactions which might impose limitations or changes which the Community is better advised to accomplish on its own initiative.

b. Incremental options

(1) Without change in the existing E.O. 11652, the DCI could issue a new DCID providing specific guidance for the application of each of the existing security categories. Such a DCID would be as definitive as the current "state of the art" makes possible in listing those types of information to which a classification of top secret, secret or confidential applies. Wide dissemination of such a list of examples would provide better guidance than is now available to those intelligence officers who are authorized to classify materials information.

(2) The DCI could indicate a recognition of complaints which have been addressed to the current application of compartments to various kinds of intelligence information and intelligence projects by issuing a new DCID which would provide guidance as to the circumstances under which adoption of a compartmented approach is justified and list the criteria which should be applied in deciding whether or not compartmentation is required.

(3) The DCI could solicit active support from departmental secretaries who have intelligence responsibilities to lend impetus to his ongoing efforts to obtain statutory authorization for the application of criminal sanctions against personnel responsible for the unauthorized disclosure of classified intelligence information.

(FLESH OUT THE INCREMENTAL OPTIONS)

c. Options for major change

(1) Formulate a new approach to the application of codeword compartments which would eliminate the use of codewords on all finished intelligence products and depend on the classification of the paper itself to indicate the degree of sensitivity of the information. Codewords would still be used within the Intelligence Community on raw information reports and on draft papers to assist analysts who need to be aware of the source of particular information as a measure of the degree of credence which can be given to the data.

(2) (This would be the new proposal on compartmentalization which is being developed by Robert Taylor, Executive Secretary of the USIB Security Committee.)

(3) Limit the use of compartment codewords only to operational aspects of particularly sensitive projects, and require DCI approval, with the advice of the USIB, for the establishment of any codeword compartmented access list.

(4) Delimit, by issuance of a new DCID, particular kinds of intelligence information or products to which no security classification is to be applied, e.g., information relating to developments in basic science.

(TO BE FLESHED OUT WITH OTHER OPTIONS)

11. Recommended DCI Course/Courses of Action

(TO BE DEVELOPED FROM CONSIDERATION OF THE VARIOUS ALTERNATIVES DESCRIBED IN PARAGRAPH 10.)

Next 2 Page(s) In Document Exempt

Approved For Release 2005/02/02 : CIA-RDP80M01133A001100090022-4