Top Secret

[redacted]

INTELLIGENCE MONOGRAPH

CRITIQUE OF THE CODEWORD COMPARTMENT IN THE CIA

CENTER FOR THE STUDY OF INTELLIGENCE

CENTRAL INTELLIGENCE AGENCY

Top Secret

TR/IM 77-02J
TCS 4530-77
March 1977

Handle via TALENT-KEYHOLE-COMINT Channels

THE CENTER FOR THE STUDY OF INTELLIGENCE IN OTR OPERATES A RESEARCH AND DISCUSSION PROGRAM KEYED TO THE PROCESSES AND FUNCTIONS OF INTELLIGENCE. THE OBJECTIVE OF THE CENTER IS TO CONTRIBUTE TO THE PROFESSIONAL UNDERSTANDING AND TO THE RECORD OF THE ART OF INTELLIGENCE. RESEARCH PROJECTS ARE UNDERTAKEN BY INTELLIGENCE "FELLOWS"—VOLUNTEER OFFICERS FROM ACROSS THE AGENCY ON FULL-TIME DETAIL TO THE CENTER. INQUIRIES ABOUT THE CENTER PROGRAM, OR COMMENTS ON THIS REPORT ARE INVITED BY THE DIRECTOR/CSI, EXTENSION 2193.

Warning Notice
Sensitive Intelligence Sources and Methods Involved
(WNINTEL)

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6

CRITIQUE OF THE CODEWORD COMPARTMENT IN THE CIA

A CRITIQUE OF THE CODEWORD COMPARTMENT IN THE CIA

FOREWORD

This study, the second in a series of Center papers on compartmentation in the CIA, focuses on the codeword compartment.* This security device is designed to provide special protection, beyond that provided by the federal classification system, to a specific category of sensitive information. Its charter is Section 9 of Executive Order 11652.[1] The Codeword compartment is only one form of supplementary protection for sensitive materials, although perhaps the predominant one. Although no exact accounting is possible, it appears that the use of codeword-protected materials may be involved in up to one-half of total Agency man-hours.

What distinguishes the codeword compartment from other forms, for example those used by the Operations Directorate to protect sources and methods, is its relatively large

---

* The first study, dated 6 December 1976, was entitled Secrecy vs. Disclosure: A Study in Security Classification. In the series of Center studies, compartmentation has been viewed as "formal" as it relates to the codeword systems, "informal" as it pertains to the generalized need-to-know found in the classification system or the more rigid need-to-know practiced in the Clandestine Service, and "bureaucratic" as it evolves accidentally from organizational phenomena. The author of the final draft of this study was [redacted] of the Directorate of Operations. He drew heavily upon the contributions of other Center fellows.

25X1A

interagency membership, its established and enduring character, its formalized procedures for granting access approvals and indoctrinating initiates, and its use of distinctive codewords to control personal access and document distribution. Usually, it protects information collected by technical means, such as electromagnetic intercept or overhead photography.

The codeword compartments--perhaps because of their size and complexity--have been extensively studied by the CIA and the Defense Department.[2] A recent Defense Department announcement described 20 ongoing studies of various aspects of compartmentation. While taking note of the earlier studies, many of which are highly technical and have a Community focus, a point was made in this paper of not covering the same ground. Instead, this study focuses for the most part on the operation of the codeword compartment within the CIA and on the criticisms of it voiced by Agency officers and bearing on the Agency's intelligence mission. The paper seeks to assess the validity of these criticisms and to suggest some remedies.

The methodology of the study involved use of an attitudinal questionnaire, interviews of officers in all directorates, and research in the available literature. For

TOP SECRET
Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6
HANDLE VIA TALENT-KEYHOLE-COMINT CONTROL CHANNELS

security reasons, the study was restricted mainly to the three principal systems of compartmentation--Communications Intelligence, TALENT-KEYHOLE [redacted] (see pages 5-7 for definitions); smaller, more sensitive informational compartments were touched on only lightly. Study of the [redacted] compartment was limited generally to information available through the [redacted] access approval. Where applicable, the intelligence product of the compartments was emphasized. [redacted] projects designed to protect the collection source, engineering development, and technology, were not included.

25X1A 25X1A 25X1A 25X1A

The study first looks briefly at the historical development of the codeword systems, spotlighting their structural and hereditary problems. It then examines the principal criticisms. A final section presents the study's conclusions and recommendations, a summary of which follows.

SUMMARY OF CONLUSIONS AND RECOMMENDATIONS

The difficulties involved in the functioning of the codeword compartments stem from the following main causes:

--the ability of agencies and departments to unilaterally establish compartments and the consequent lack of central control over them;

--the unilateral withholding of compartmented information by the originator of the information;

--the failure of the compartments adequately to distinguish between the needs of analysts and ultimate consumers;

--the fragmentation of intelligence caused by the operation of the varied compartments; and

--the failure consistently to decompartment nonsensitive information.

The study's recommendations fall into two broad categories: those within the competence of internal CIA management to act upon and those affecting the Intelligence Community as a whole. The former deal with:

--centralizing record keeping on access approvals of all sorts;

--the creation of an Agency information center to assist researchers and others whose jobs require access to compartmented information;

--CIA leadership in the updating and/or preparation of guidance manuals for the three main compartments;

--improved security, indoctrination, reindoctrination, and a new emphasis on substantive indoctrination;

--suggestions for the bulk decontrol of imagery eligible for decontrol; and

--establishment within a CIA Classification Board of a special section on compartmented information.

To provide central supervision of the national compartments, the study recommends the revision of Section 9 of Executive Order (E.O.) 11652 to require: (a) the concurrence of the Director of Central Intelligence (DCI) whenever a member of the Intelligence Community establishes a compartment that inhibits the flow of information to other members of the Community; (b) DCI monitoring of the existing compartments to ensure that they do not impede the production of national intelligence.

To cope with the problem of decontrol of compartmented information, the study recommends:

--a mandatory annual review of compartmented information to segregate for decontrol information whose sensitivity has changed during the year;

--appointment by the DCI of a committee or task force to study the desirability of decompartmenting to SECRET NOFORN the totality of the TALENT-KEYHOLE (TK) imagery product; and

--decontrol to SECRET NOFORN or CONFIDENTIAL NOFORN, as appropriate, of all but the most sensitive [redacted] Communications Intelligence (COMINT).

25X1A

To counter the fragmentation of intelligence, the study recommends the establishment within the DCI Committee

structure of a new Committee on Integrated Intelligence. It also makes several recommendations for structural reform suggesting that:

--the Agency sponsor legislation for the establishment of a new category of legally protected information to be called: Sources-and-Methods Information;

--the DCI and the Intelligence Community abolish all existing compartments and replace them with one uniform Sources-and-Methods Compartment. (Access to this information would require a full background investigation.); and

--formal criteria for need-to-know be drawn up for collector, top policy maker, analyst, processor, and consumer. All Sources-and-Methods Information would be slugged to reflect these criteria and routed accordingly.

TOP SECRET
HANDLE VIA TALENT-KEYHOLE-COMINT CONTROL CHANNELS

THE CODEWORD COMPARTMENT

"We should also intensify our efforts to downgrade, sanitize, and decontrol where possible highly compartmented products so that they may be more widely disseminated and used. This will require greater refinement in distinguishing categories of intelligence which must be given greater, rather than less, protection in such a new atmosphere."

Director of Central Intelligence
Perspectives for Intelligence 1976-1981.

Genesis of the Codeword Compartment

The Hoover Commission in 1955 remarked that the CIA might well owe its existence to the surprise attack on Pearl Harbor. That most disastrous of intelligence failures was due in no small measure to the mishandling of compartmented intelligence. The dissemination of decrypted Japanese communications, codenamed [redacted] was so restricted that the theater commanders in Hawaii did not regularly receive them. The decrypted items were not synthesized into a meaningful whole nor collated with information from other sources.

25X1A

The embryonic compartment that handled the Japanese communications was managed by the War and Navy Departments. In 1941 the Navy decryption unit, the Communications Security Unit, had a total staff of 300; the Army unit, the Signal Intelligence Service, a staff of 224 in Washington and 150 in the field. A G-2 agreement with the Office of Naval Information (ONI) of 23 June 1941 on the dissemination of COMINT designated only nine persons as recipients--essentially the top civilian and military officials concerned with national security. By the end of the war, in Washington alone, the Army unit had a staff of over 10,000 and the Navy unit one of 6,000.[3] Thousands of others were recipients of the product. The pattern of rapid growth thus established continued for many years.

COMINT became a formal compartment in the modern sense of the term with the signing of a [redacted] agreement in 1946. This agreement established procedures on both sides for the handling, safekeeping, and exchange of COMINT. It was an outgrowth of the wartime exchange of COMINT: our [redacted] the codename for decrypted German traffic.

25X1A

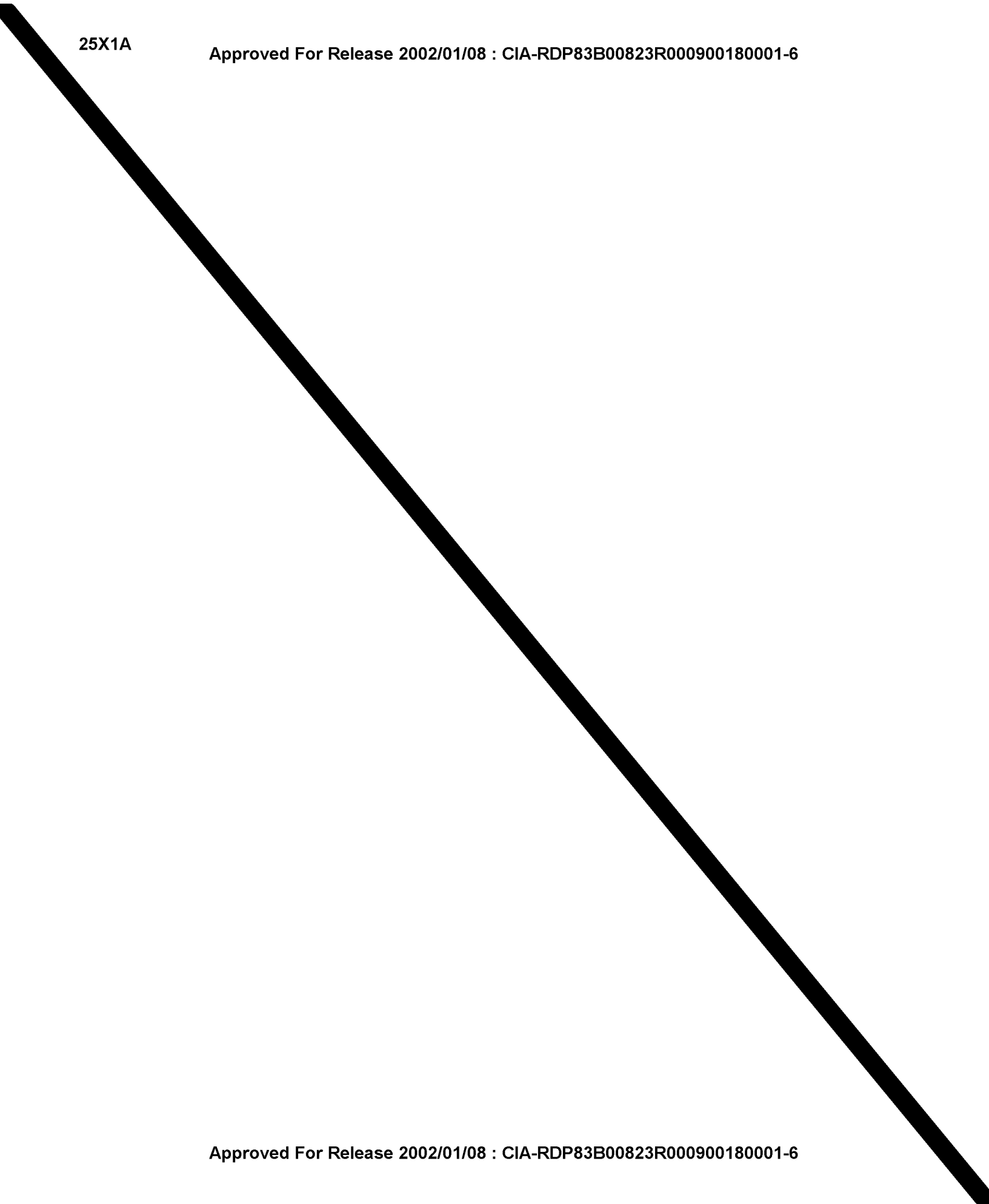
25X1A

In 1952, the responsibility for COMINT was centralized in the newly created National Security Agency (NSA) to help

TOP SECRET
HANDLE VIA TALENT-KEYHOLE-COMINT CONTROL CHANNELS

eliminate the duplication in intercept and dissemination efforts between the various collectors that had been a problem from the beginning. But even then COMINT was not considered foreign intelligence (in the sense of being part of the foreign intelligence collected by the U.S. intelligence effort). This did not change until the establishment in 1958 of the United States Intelligence Board (USIB--now the National Foreign Intelligence Board--NFIB) under the chairmanship of the DCI, when COMINT at last became a recognized part of foreign intelligence.

Technical advances in collection capabilities brought forth new compartments, vaguely patterned after the COMINT compartment. CIA's use of the U-2 aircraft for high-altitude photographic coverage led, in the mid-1950's, to the establishment of the TALENT compartment to protect both the collection system and its intelligence product. A Presidential directive of 20 August 1960 broadened the TALENT Control System to include all information collected by means of nationally tasked aerial reconnaissance, at the same time creating a subcompartment, codenamed KEYHOLE, for information collected by satellite. By 1962, the problem of managing the development and operation of the growing satellite systems and of administering access approvals to information



Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6

superintending satellite collection of photographic and signals intelligence; and TALENT-KEYHOLE containing the
25X1A intelligence product of [redacted] Although not divided functionally between collection system and intelligence product, the COMINT compartment is stratified into three categories,
25X1A based on sensitivity. [redacted] is the most sensitive.

Standing by the side of the three main compartments are an "indeterminate" number of lesser compartments. Members of the former Intelligence Resource Advisory Committee (IRAC) were said to require access to some [redacted] compartments 25X1A to do their jobs. But the exact number of compartments in the Intelligence Community at any given time is not easy to ascertain since it is difficult to find anyone who is cleared for all of them or even witting of the existence of all of them. There is no central point in the Agency where one may go to verify the access approvals held by an individual. The Compartmented Information Branch of the Special Security Center maintains records of the three main systems and some third country ones only. Control officers for the other compartments are dispersed throughout the Agency. Most, if not all, of the creation of the smaller compartments appears to have occurred within the Defense Department.

CIA and the Codeword Compartment Today

The codeword compartments today are vastly different from the wartime compartment out of which they grew. The main differences lie in the numbers of employees with access to them, in the complexity of their structures, and in the vastness of their information holdings. All three major compartments have grown steadily, and their scope will further expand with the advent of "real time" collection. Each advance in collection technology has brought a corresponding increase in the numbers and categories of persons with a "need-to-know" the information collected. This increase has even transcended the Intelligence Community. Witness the contributions of overhead photography to agriculture, climatology, exploration for new energy resources, and drought control.

In 1975, the Office of Central Reference (OCR) disseminated more than four times as many compartmented as noncompartmented intelligence reports (444,870 versus 98,551). The Intelligence Community's output of compartmented finished intelligence (monographs and articles) handled through OCR exceeded that of finished noncompartmented intelligence by 14,359 to 9,742. Although these figures do not represent the complete output of either the CIA or the Intelligence

Community, they give an accurate picture of the relative numerical significance of compartmented intelligence reports and documents. To process the latter, large numbers of CIA employees have been admitted to the compartments. Thus, 86% of all employees have access approvals for COMINT, 60% for

25X1A

TK, and 40% for [redacted] Large segments of the Agency, particularly in the Deputy Directorate of Intelligence (DDI) and the Deputy Directorate of Science and Technology (DDS&T), work almost entirely on compartmented intelligence. And even in the Deputy Directorate of Operations (DDO), where most divisions spend relatively little time on it, one whole

25X1A

division, [redacted] works nearly full-time on COMINT. Probably one-half of total Agency man-hours is spent on some facet of compartmented intelligence. The size of this investment underscores the importance of understanding the compartmented milieu within which such a large volume of sensitive but valuable intelligence is collected, processed, evaluated, and disseminated.

Despite the relatively large access of Agency employees to compartmented information (at least to the main compartments), complaints are still heard from analysts and others

---

* Since February 1977, part of the DDS&T.

TOP SECRET
HANDLE VIA TALENT-KEYHOLE-COMINT CONTROL CHANNELS

of production difficulties caused by denial of codeword information. At least in the minds of many analysts, the problem posed by Pearl Harbor is still with us: How do we reconcile the protection of highly sensitive information with its optimum use? And on the side of optimum use, an old question with new ingredients: What is the effect on the intelligence cycle of the multiplicity of unilateral compartments with their collection orientation, their overlap, and their rigidities? A related question is whether there really is an intelligence gap caused by the compartments.

For this study, the attitudes of a cross section of Agency employees toward compartmentation were surveyed.[6] Although the 163 persons who answered the questionnaire did not technically qualify as a "random sample," they constituted a representative sample in terms of directorates, job categories, grades, and length of service. One hundred and thirty-one had access to at least one compartment and 78 to more than two. What should be stressed is that 73% of the respondents, a very significant percentage, said they had not been denied codeword information; on the contrary, they had received it regularly on a need-to-know basis. Overall, the survey conveyed the impression that the codeword compartment was not a serious problem for the CIA.

But detailed interviews with persons intimately concerned with the compartments left a somewhat different picture. Although not contradicting the survey as such, the picture was of a much more variegated, more complex landscape, dotted here and there with problems stemming from the operation of the compartments. For the most part, these problems involved the operational dynamics of the compartmented systems, such as:

--the anarchic nature of the codeword compartments;

--the unilateral withholding of compartmented information;

--the failure to distinguish between the needs of analysts and ultimate consumers;

--the fragmentation of intelligence; and

--the failure to decompartment nonsensitive information.

In the sections that follow these issues are discussed.

THE ANARCHIC NATURE OF THE CODEWORD COMPARTMENT

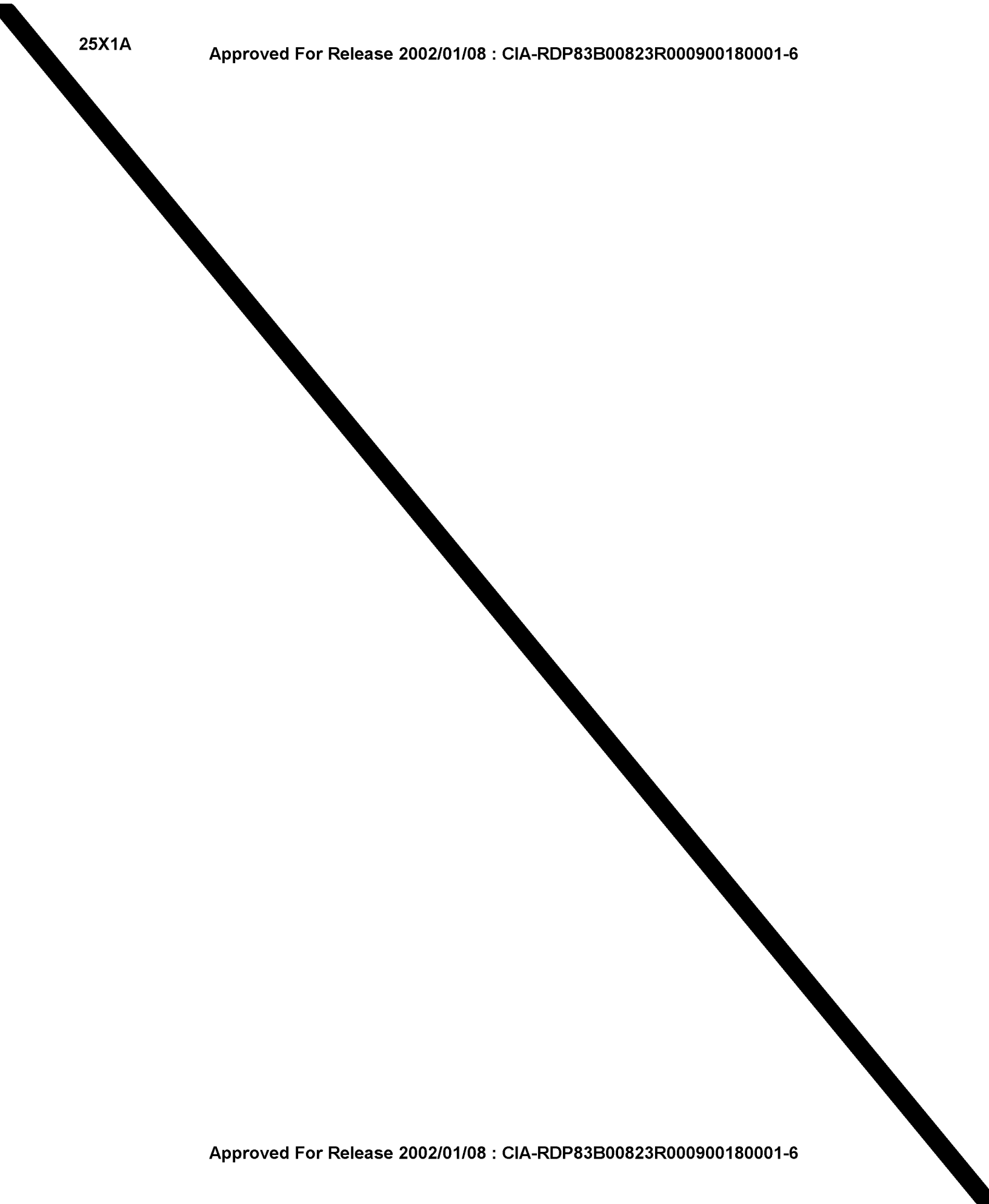
Lack of Central Control

The unilateral authority of the agencies to establish compartments permits the originating department to fence off its information and establish ground rules for access and distribution. In the name of security, information may be

withheld in whole or in part, watered down by sanitizing, or served up as a restricted summary. There are, of course, DCI committees that attempt to coordinate the use of compartmented information and impose order in an area where autarchy is too often the rule. But the originating department remains the final arbiter. No wonder then that the compartments are dissimilar in structure, conflicting, and overlapping.

Nor is it surprising that they generate confusion. Each "subcompartment" in the [redacted] compartment has its own guardian codeword. Even if an officer possesses the generic [redacted] for access to the complex, he does not enter a particular subcompartment without a specific access approval for the subcompartment. If one had business with all of them, it would require a half dozen or so access approvals. Each codeword, except [redacted] protects a specific photographic or Signals Intelligence (SIGINT) satellite collection system. Each collection project is singlemindedly focused on the development, production, or operation of its own system. Its preoccupations are those of the designer, engineer, or system manager, not those of the processor, analyst, or consumer. The interests of the latter, therefore, tend to be neglected. Information belonging by definition

25X1A 25X1A 25X1A



Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6

and an unclassified designator [redacted] assigned by NSA. 25X1D
This can confuse the user of the intelligence product, making it difficult for him to remember which designator applies to which system. Whether the designators bolster security, as originally intended, seems questionable. These examples are meant to suggest rather than exhaust the degree of confusion obtaining in the compartments. As the number of access approvals held by an individual increases, it becomes more difficult for him to distinguish one from the other or even to remember clearly those he holds.

A product of the confusion factor is the compartmentation expert. The intricacies of compartmentation are such that few can weave their way through its recesses without a guide. To publish compartmented information more widely, it is necessary either to sanitize or to decompartment it. And it is here that the services of the compartmentation expert are in greatest demand. The analyst must sometimes consult with him to verify that finished intelligence has the proper markings and conforms to the rules of compartmentation. This can introduce additional delay into the production-dissemination process. But the experts, located for the most part in the Requirements and Evaluation Staff in the Comptroller's Office, are not exempt from confusion. They

tend to be highly specialized, and when a compartmentation problem involves information moving simultaneously in two or more compartments, they are sometimes hard put to unravel its complexities. This is no reflection on them, but rather a consequence of the structural incompatibility of the compartments and the inadequacies of existing guidance, particularly for sanitizing and decompartmenting.

Psychological Aspects

We know that secrecy by its very nature may affect the personality of its practitioners. This is true of all forms of secrecy from the primitive secret society to the codeword compartment. The latter is a heightened form of secrecy that resembles the former in many ways. It has the aura of a secret society. It has its initiation, its oaths, its esoteric phrases, its sequestered areas, and its secrets within secrets. And in place of passwords and hand signs, there are letter designations on badges. There are in-groups and out-groups. No wonder, then, if the codeword compartment has unintended psychological effects.

For many, the badge with its distinctive letters has become a status symbol, and for some of them the symbol has fused with careerism. Others, equating knowledge with power, have become collectors of clearances. They have lost

sight of need-to-know. The effect on those without access to a compartment is sometimes adverse. They may wonder if their loyalty is being measured against those admitted to the compartment. The aggressive analyst who considers it a point of honor to know everything going on in his field may take exclusion as a challenge to outwit the codeword compartment. He feels free to probe and to exploit to the hilt his personal contacts. In this sense, compartmentation tends to subvert the formal channels of communication. Whether aggressive or not, the analyst who knows he is not privy to compartmented information on a particular subject will often be more diffident in expressing his views. And if his interlocutor retorts: "You don't have all the clearances," his diffidence may increase.

There are also other more general effects. Some are so impressed with the trappings of codeword information that they come to consider it more accurate than other information not confirmed by COMINT or photography.[8] Others see codewords as an attention-getting device, pyramiding them on publications to assure the customer that all sources have been tapped, thus contributing to overclassification and overcompartmentation. Some components of the Intelligence Community--NSA is often accused of this--compartment infor-

mation according to its substantive importance rather than its intrinsic sensitivity. Those admitted to codeword compartments frequently believe they have been granted a certified need-to-know for everything within the compartment. Still, codewords do deter: few would have the temerity to take codeword material home, few even among those who take home other types of classified material. On balance, however, the psychological side effects of the codeword compartment seem to diminish rather than enhance security.

Problems With Other Agencies

The interests of the department or agency originating and administering the compartment and those of the departments receiving the information contained in the compartment are not the same. Differences arise most frequently over the number of persons to be admitted to a compartment and over the kind and amount of information to be granted to those admitted. The DCI Committee structure takes the edge off these disputes, establishes a modus vivendi, but has been unable to remove their causes. Because of CIA's strong position with respect to the TK and [redacted] compartments, CIA access to these compartments is usually not a problem. 25X1D

Unfortunately, the same cannot be said of the COMINT compartment nor of some of the smaller Defense Department compartments, particularly those of the Navy.

With respect to the COMINT compartment, CIA's problems on the substantive side generally involve the difficulty of obtaining what some analysts believe is a full enough text of the actual intercepted messages rather than the gists, summaries, or paraphrases that the National Security Agency prefers to make available in some cases. These difficulties extend to disputes over what constitutes "technical data"--the material associated with the intercept which describes in essence the "sources and methods" part of its origins. Some CIA analysts feel that they need more of the latter in order to make full use of the intercepts, while NSA naturally wants to protect it, especially in the light of the bad leaks of intercepted communications which have occurred in the media in recent years. It is this concern which also generally formulates NSA's policy in substituting gists and summaries for full texts of COMINT material.

Judging the right and wrong of these positions is almost impossible at present except on a case by case basis. It is clear, however, that the organizational and jurisdictional boundaries thrown up around the compartments by

TOP SECRET
Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6
HANDLE VIA TALENT-KEYHOLE-COMINT CONTROL CHANNELS

the intricate rules and semi-independent ability of the agencies to construct these rules have contributed in no small measure to the situation and that any reform must go in the direction of centralizing the authority for establishing national compartments and the rules under which they operate.

Two of the Navy compartments may be taken as typical of the problems posed by the smaller national compartments. These compartments (unidentified here for security reasons) have the trappings of the three main compartments--codewords, indoctrination oaths, and special transmission channels. But they also have distinctive features being functionally tiered into levels for collection, analysis, and production. The corresponding tiers require separate "tickets" for access. CIA's principal difficulty with these compartments lies in the restricted number of "billets" or access approvals it receives. This allotment of "billets" is clearly not based on a careful assessment of need-to-know within the Agency. According to one estimate, the Electronics Intelligence (ELINT) activities in the Agency presently require a tenfold increase in the number of "billets" in one of the compartments. Since there are not enough "billets" for all the analysts who need them, the practice of juggling per-

TOP SECRET
Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6
HANDLE VIA TALENT-KEYHOLE-COMINT CONTROL CHANNELS

sonnel in and out of the compartments, briefing and debriefing them, has developed, offering a good example of compartmentation defeating its own purposes.

What NSA and the Navy are doing, according to their point of view, is unilaterally protecting some of the most sensitive and fragile information the U.S. possesses. The culprit is the unilateral nature of the compartments; only a central arbiter can resolve the differences.

Structural and Conceptual Problems

In the preceding section, some of the ways policies and procedures imposed by compartment managers can adversely affect the raw and finished intelligence product was described. The compartment in its origin is the creature of the collector. It reflects his two principal concerns: to protect the collection system and to maximize collection. It is only when these concerns conflict with the ultimate purpose of all collection--the production of national intelligence--that a problem is created.[9] Unfortunately, the collection bias of the compartments sometimes does just that.

Compartmental bias expresses itself structurally in the establishment of separate collection and product compartments for the same system. The classic instance is the [redacted] 25X1A

collection compartment and its TK counterpart. The underlying assumption is that the Intelligence Community can be neatly divided into collectors and consumers. But, suppose an analyst has received an unconfirmed clandestine intelligence report about a new missile system. He knows overhead reconnaissance can confirm or deny the report. But to task the appropriate system, he must have at least a nodding acquaintance with the collection projects. If he received photographic coverage and the results are inconclusive because of the sun's angle, both he and the processor (the photointerpreter) must know that it is possible to request additional coverage at a different time of day. Only the collection system operators need know how this is done, but the processor and the analyst must know that it can be done and be able to task the system.

Ignorance of the potential of overhead photography as a means of solving intelligence problems and of supporting military and foreign policy decisions is still fairly widespread. For example, relatively few State Department personnel are cleared for TK. It was only within the last year that State got around to establishing [redacted] for the storage of TK and the use of those cleared for it. There have been instances when the use of overhead photography in

25X1A

analysis would have been useful but, being unfamiliar with its availability, analysts did not think to ask for it.

Besides analysis and production of finished intelligence, the analyst is sometimes responsible for evaluating the raw product of the collection system. To do the latter, the analyst must sometimes know more about the collection system than is normally provided by access to the product compartment.

What has been said of overhead photography is equally true of overhead SIGINT. The processor (the signals analyst) and the finished intelligence analyst need to know less than the collector but more than the consumer of finished intelligence. The latter needs to know that the system exists or will exist, its intelligence potential and its reliability, but not the processes employed by the systems operator, the processor, and the analyst.

Although not divided structurally, the COMINT compartment is nonetheless split along user-collector lines. The practices of gisting and withholding "technical data" mentioned in the preceeding section are predicated on the principle that message externals, the verbatim text, and the means by which the information was collected and processed should be kept in the hands of the collector and not released

to the user. The separation of "technical" COMINT from that released to users takes place by means of need-to-know rather than by means of formal compartmentation. Regardless of the means employed, the effect on the analyst is the same. Whether the bias is structural or conceptual, it has this in common: it does not fully accommodate the intermediate need-to-know situated between the collector and the consumer of finished intelligence.

FRAGMENTATION OF INTELLIGENCE

All forms of compartmentation have a fragmenting effect on information. But the codeword compartment, because of the volume and importance of the information sequestered, undoubtedly has the greatest effect. Not only is all information on one subject not in one file, but access to each repository requires a separate access approval. The principle that assigns information to a particular compartment is not a fully logical one; it is based primarily on security and the convenience of the collector. Intelligence, like all knowledge, ideally is seamless and indivisible. In its search for meaning it abhors all compartments, no matter how necessary they may be.

How serious is the fragmenting effect of the codeword compartment? [redacted] a military and warning analyst, answers the question this way: 25X1A

> The compartmentalization of information--both intelligence material under special clearances and policy or operational information by executive action--is a serious enough problem in normal circumstances. In time of possible impending hostile action, it could be disastrous. The gulf which separates the Joint Chiefs of Staff from the desk-level military analyst may be immense . . . . From day to day it may not make much difference whether or not the analyst is privy to much of this material (in very restricted collection systems); he may make some minor skips for lack of it, but the security of the nation will not be at stake. But it is entirely different when the enemy is getting ready for some surprise action, for then the analyst's "need to know" may be as great, if not greater, than that of the policy maker.[10]

Indeed, it is arguable that all intelligence failures, starting with that of Pearl Harbor, are attributable in some degree to abuses of compartmentation, to a failure to integrate information. According to [redacted] "The intelligence analyst who did not know that the Pueblo was off North Korea prior to its seizure, and most did not, was not likely to have alerted his superior to some anomaly in North Korean naval activity. The list of such examples is endless."[11] 25X1A

Conspiring against the integration of information in the Agency is not merely the codeword compartment but also the information explosion itself, the increasing special-

ization among analysts, and the functional organization of the DDI and DDS&T.[12] One consequence is the increasing difficulty of assembling all needed information on a given subject. Although there is a plethora of indices, few of them are all-source. When intelligence data are not entered into compatible computer programs, the computer is unable to perform its unique function of bringing together related but dispersed fragments of information; there is a loss of "convergence." The basic information on lasers lay dormant in the Intelligence Community, no one knowing it was there, until a concerted effort was made to find it. Recently, a team [redacted] had difficulty getting the information it needed out of some of the more hermetic compartments. Some Agency officers believe that the latter not only reduce the flow of information to a trickle, but channel it in directions contrary to need-to-know. Sensing this situation, the DCI in his Perspectives for Intelligence: 1976-1981 called for a more integrated approach to intelligence: "The growing interdependence nationally and among disciplines will require a greater integration of many activities which in prior years could be handled in separate compartments."

25X1D

The mischievous effects of fragmented data also affect requirements, collection, and dissemination. For example,

the Fiscal Year 1975 performance report on Key Intelligence Question (KIQ) 14 [redacted] concluded that: "Where data were disseminated widely enough to permit coordinated tasking, collection tasks were substantially or almost completely satisfied." The report explained that compartmentation of "certain relevant data" (pertaining to [redacted] had hampered Community efforts to collect and disseminate information concerning the requirement; exploitation and tasking feedback had suffered for the same reason. The report added that although the problem "has been alleviated in part by wider distribution of certain of the relevant data . . . there still remains the difficulty of disseminating to the interested customer meaningful finished intelligence on these data." In order to exploit and analyze available information on one aspect of KIQ 14, the report suggested this could probably be done "if all-source data--some of which is highly compartmented--were exploited by an analytical group." But here again, because of the restrictions governing the particular compartment, the analytical group would have had difficulty getting the results of its work to appropriate customers.[13]

Since the compartments are organized around a technique of collection, the information they contain is there because

it derives from that technique, not because it constitutes a discrete body of knowledge that can stand on its own feet. The information in the various compartments is therefore incomplete and only becomes fully meaningful when synthesized and meshed with collateral and other compartmented information. This is obvious to all analysts. But for a variety of reasons, some of which have already been mentioned, the full integration of intelligence data still eludes the Intelligence Community. This is particularly so in the area known as "fusion," the coordinated use of different collection techniques to obtain a rounded view of a single "event."

Perhaps in no other area are the barriers of compartmentation so formidable. For fusion demands close intercompartmental--and therefore interdepartmental--coordination. Multitechnique collection and subsequent integrated analysis of the products is not one of the strong suits of the Intelligence Community. The physical and administrative dispersion of the processing elements may compound the difficulty, although the simple amalgamation of organizations is by no means an easy answer to what may be more a matter of attitude and perception than of structure. NSA does the readout for COMINT, ELINT, and telemetry; the ELINT

unit of CIA does the readout for ELINT and telemetry collected by CIA or received from third parties; the National Photographic Interpretation Center (NPIC) does the readout for overhead photography, [redacted] 25X1D and the Office of Computer Services assists both the ELINT unit of CIA and NPIC in their readout.[14] 25X1D

Advances in technology are thus putting strains on the traditional compartment. To remedy this, some have proposed the establishment of a multisensor compartment. In the interim, the National Intelligence Officer (NIO) system, the KIQs (which ignore compartments), and the pioneering concept of the [redacted] 25X1A are integrative forces acting to counter the fragmentation of intelligence.

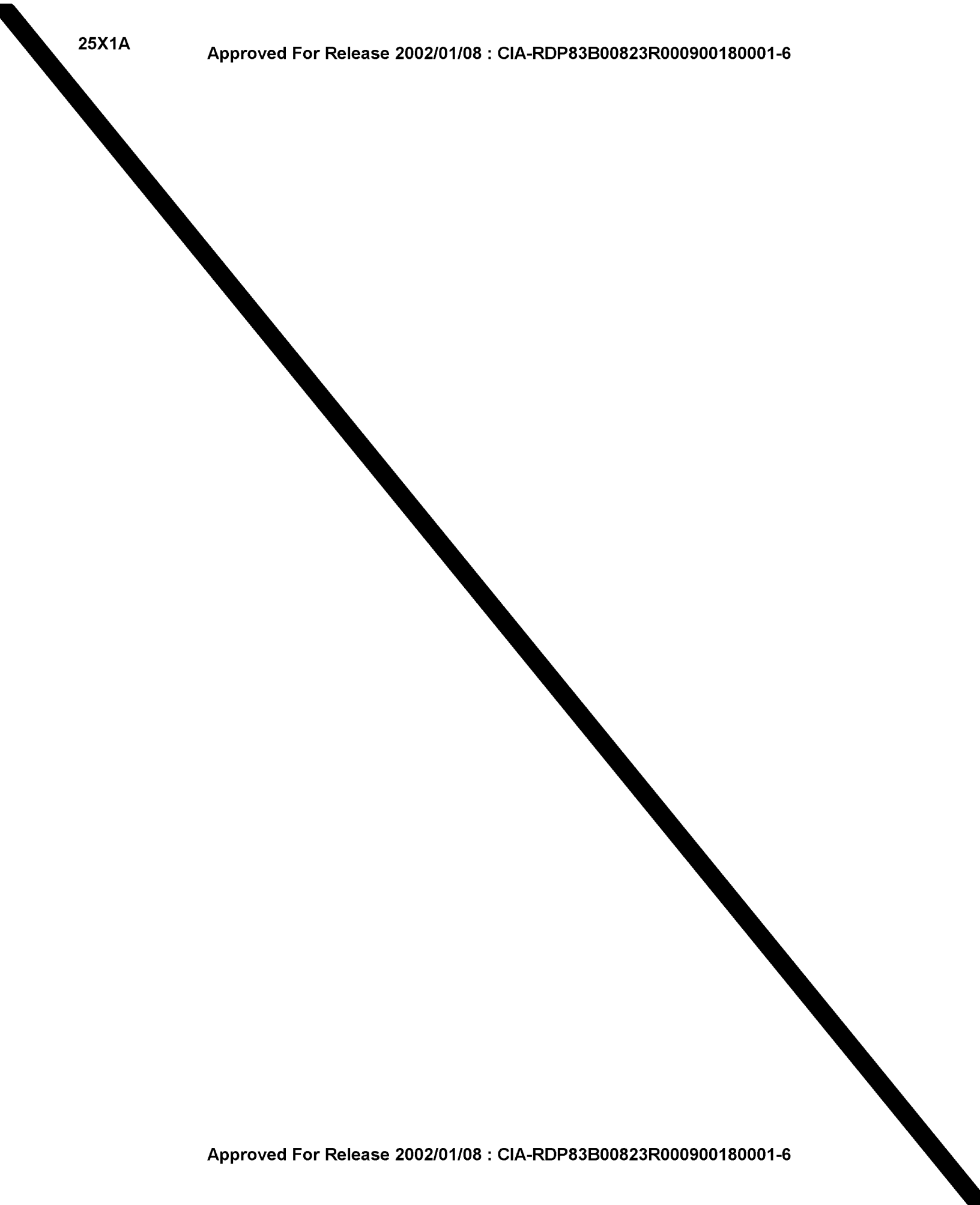
Decompartmentation

Decompartmentation or decontrol is the removal of information that has undergone a change in sensitivity from the compartmented state to the simple protection of the federal classification system. As such, it is an important measure of the health and legitimacy of the codeword compartment. In terms of the intelligence process, if properly conducted, it fosters the integration of intelligence. On the other hand, it is often controversial, triggering dis-

putes over the residual sensitivity of a piece of information, the extent of foreign knowledge of our technical collection systems, and the risk of compromise if the information is decontrolled. In arguing these points, opponents and proponents often reason as if decontrol were tantamount to declassification.

In assessing how decompartmentation is functioning, it is necessary to note at the outset that there is no mandatory review of compartmented information for purposes of decontrol. The latter usually takes place only upon request, when someone has noticed a nonsensitive item that would be useful to analysts not enjoying access to the compartment. Under these circumstances, overcompartmentation and overclassification are inevitable. The COMINT compartment is a case in point. An earlier Agency study of compartmentation concluded: "We are compartmenting an unnecessarily large volume of intelligence and intelligence information, notably COMINT products, the bulk of which has in effect been sanitized when published by the Cryptologic Community."[15] The study explained that most "COMINT information is passed to consumers in the form of combined, multiCOMINT source reporting." This, the study stated:

TOP SECRET
HANDLE VIA TALENT-KEYHOLE-COMINT CONTROL CHANNELS
Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6



Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6

25X1D

Since it is difficult to determine the probability of unauthorized disclosure of any kind of information, compartmented or not compartmented, most discussions of the risks of decompartmenting end up as judgments concerning the relative sensitivity of a piece of information and the probable effects of its unauthorized disclosure. The only official measure of sensitivity is the three levels of the federal classification system corresponding to degrees of damage that unauthorized disclosure would cause to national security: simple "damage" for Confidential, "serious damage" for Secret, and "exceptionally grave damage" for Top Secret. These three levels equate to the "probable effects of disclosure." Through a study of the latter, we arrive at

the proper classification of a piece of information. We can, as a rule, decompartment to the Top Secret collateral level without any loss of protection. In fact, the [redacted] study concluded that "there is less control of documents classified Top Secret when handled in COMINT control channels (and to a lesser extent in TK channels) than would be the case if given the same classification and not compartmented."[19] Normally, decompartmentation is to the Secret or lower level, reflecting a corresponding decrease in the sensitivity of the information decompartmented. The argument sometimes heard that decontrol "tends to increase the flow of information toward the public domain" is a specious one that ignores the classification system. Almost equally specious is the contention that we should not decompartment to the Secret level because many holders of a Secret clearance have not had a full background investigation. To the extent this contention has merit, it argues for changing the clearance requirements for Secret or limiting certain categories of Secret information to those who have had a full background investigation. In the meantime, E.O. 11652 is the only operative guidance.

25X1A

The notion that some compartmented information, such as [redacted] COMINT, is eternally sensitive and therefore

25X1A

TCS 4530-77

automatically exempt from downgrading or decompartmentation finds no basis in E.O. 11652. Compartmented information is just as subject to mandatory review after ten years upon request and to compulsory 30-year review as any other type of classified information. Yet, COMINT regulations do not envisage the possibility of decompartmenting [redacted] 25X1A information except in the military context in wartime.[20] Nor is there any provision for decompartmenting [redacted] 25X1A information. The decontrol of TK information is in the hands of a subcommittee of the DCI Committee on Imagery Requirements and Exploitation (COMIREX) which is more attuned to the [redacted] 25X1A collectors than to the TK users.

On the other hand, there are secrets connected with overhead reconnaissance which must be protected. They concern the advanced technology of the systems and their collection capabilities. 25X1A These are the secrets that the [redacted] and TK compartments protect. But do all these secrets require supplementary protection or would simple classification suffice for some or all of them? The answer hinges to a great extent on how much the Soviets already know about our capabilities and what, if anything, they could do and would do, if they knew more. There is no doubt that the Soviets are acutely aware of our overhead recon-

Next 2 Page(s) In Document Exempt

Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6

thousands of analysts, researchers, and contractors who are cleared for Secret only. A senior CIA analyst has observed that the Army's Training and Doctrine Command, which draws up training doctrine for the future, is largely ignorant of Soviet capabilities and needs the relevant compartmented intelligence. Large numbers of Defense Department technicians are striving to counter Soviet weapons systems without being privy to compartmented information on the subject. Stepped-up decompartmentation would improve the quality of analysis among Defense and other contractors. Counting the tactical commander, there is therefore a large, untapped market for decompartmented or sanitized intelligence, one that will probably expand greatly with the advent of real-time systems.

Closely allied to decompartmentation is sanitization, an alternative means of removing information from the code-word compartment. It also involves a calculation of the degree of sensitivity, but, more particularly, it requires explicit knowledge of what constitutes the sensitivity of a given piece of information. This may be the source or the method of collection or exploitation, the source-revealing nature of the content, or some combination of these. The job of sanitization is to delete or obscure the sensitive elements adhering to the information. "Sanitization is

accomplished by deliberately changing the original material through a process of synthesis with other source materials or by additions or deletions of substance. A prerequisite of sanitization is the existence, or a reasonable presumption of the existence, of separate and logical but less sensitive sources or methods."[28] It has been estimated that from one-fourth to one-third of the original information may be excised. The result is often a significant loss.[29]

But sanitization, which is inherently difficult and time-consuming, is made even more so by the lack of precise, up-to-date guidance. The TK control manual dealing with sanitization was issued in 1956; the [redacted] control manual issued in 1966 makes no provision for decontrol; the Communications Intelligence Security Regulations (CISR) contains no guidance on sanitization, although it provides for decompartmentation of military information in time of war, and authorizes the publication of [redacted] information in a separate NOFORN series. There are CIA compartmentation experts who provide invaluable guidance on knotty questions, but the bulk of sanitizing must necessarily be done by analysts. Typical perhaps of the approach to sanitizing of most officers is the technique of two experienced analysts interviewed for this study. Because of the lack of precise

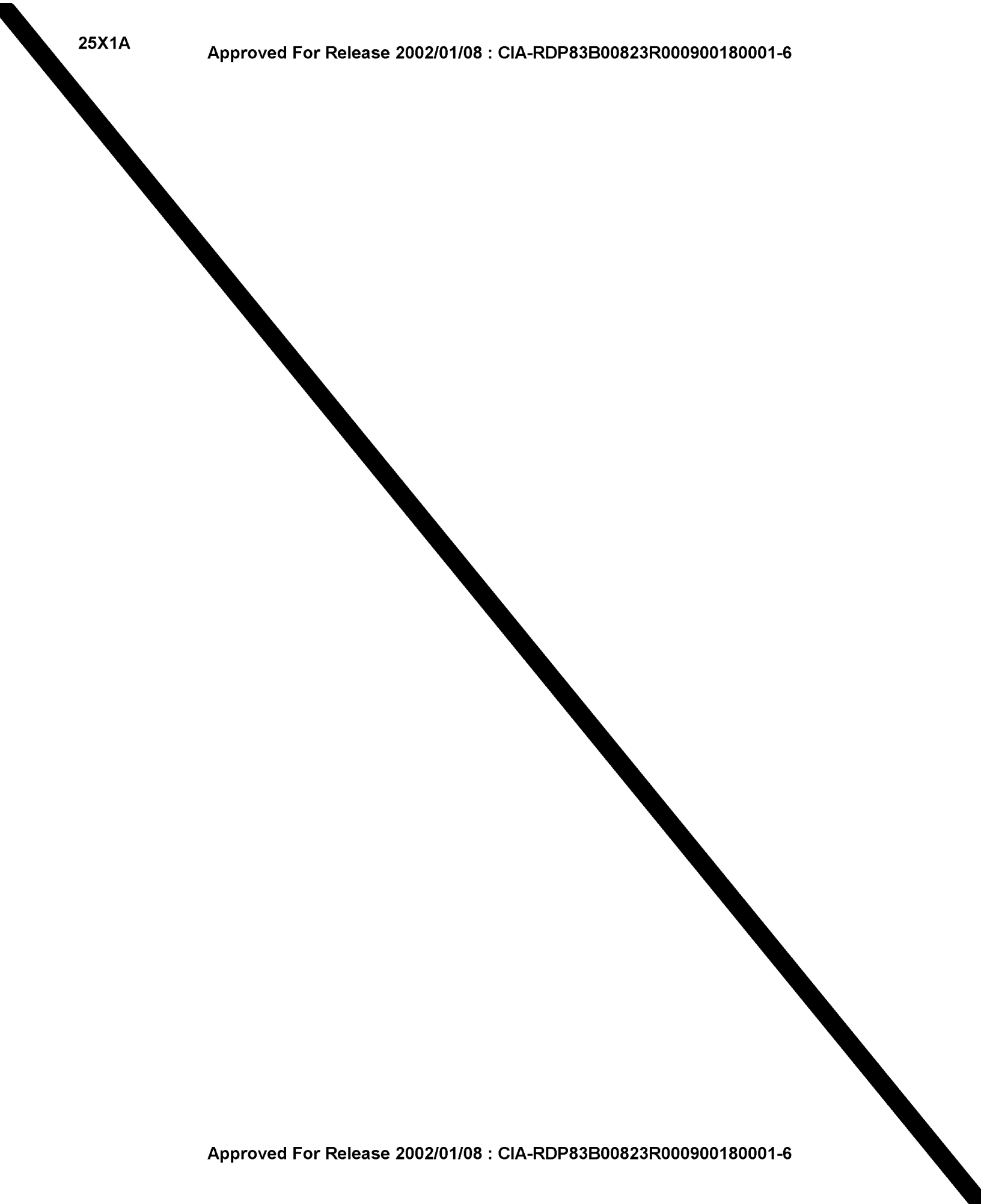
25X1A

25X1A

guidance and the pressure of deadlines, they "play it safe," and without regard to any specific criteria, quickly cut out everything that looks sensitive. A more considered approach might reduce significantly the percentage of information excised and the corresponding loss of substance.

Because of the cost and time factor, sanitization is clearly not a substitute for the bulk decompartmentation of eligible material. The latter approach is the only economical, timely means of getting large quantities of information to those who need it but lack access to it in the compartment. Despite a failure to follow through on the full intent of the Presidential directive, great progress

25X1A



Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6

intelligence compartment." Once admitted to the latter, need-to-know would determine further access. One senior officer interviewed called for the abolition of all codeword compartments, the imposition of stiff penalties for disclosure, and the use of only these five designators: CONFIDENTIAL, SECRET, TOP SECRET, NOFORN, and TOP SECRET

25X1A [redacted] Others saw no problem in combining COMINT and TK into a single compartment. A leitmotif of military studies of compartmentation has been emphasis on the "gap between the sensor community and the weapons applications community" which has been preventing combat commanders from receiving needed information.

A recent study by the former USIB Security Committee

25X1A [redacted]

recommended replacing the present system with two compartments, one for technical data (collection data) and one for the product of collection. "Efficiency and utility," the study said, "would seem to indicate the establishment of a single system of access based strictly upon intelligence needs once personal eligibility is determined. The local senior intelligence officer is best qualified to determine intelligence needs. Therefore a single system of product compartmentation should be established using the current

personnel security standards with decentralized access granting authority." There is thus something approaching consensus on the need for a unified system in which need-to-know would play a greater role than now. The nemesis of proposals for reform of so complex a thing as the codeword compartments is that what looks simple in theory may be confusing in practice. Thus, the [redacted] scheme replaces 25X1A old codewords with new ones and substitutes internal compartmentation for external. And the single unadorned compartment fails to come to grips with the complexities of routing sensitive information throughout the Community. A synthesis of the best features of these various proposals may nevertheless be possible.

CONCLUSIONS AND RECOMMENDATIONS

A high percentage of CIA employees enjoys access to at least one of the three main compartments. Generally, 25X1A employees feel they are receiving compartmented information in accordance with the need-to-know principle.[31] The [redacted] complex comes closest to being a problem. Some 40% of Agency personnel have access to one or more of its "compartments," but this is a differential access that does not

always meet the needs of analysts. Even when it does not exclude, this partitioned compartment confuses, acting as a drag on the intelligence process. One may rightly ask whether its structure is not more responsive to the requirements of managerial convenience than to those of security. Overall, the relatively broad access to compartmented intelligence enjoyed by Agency employees has apparently not caused significant security problems.

There is a problem of access to the smaller Navy compartments and a problem of access to adequate substance in the materials in the compartments. By fragmenting intelligence data, by overcompartmenting, by hindering computer retrieval and convergence, by complicating the fusion of information collected by different techniques, the compartments have made more difficult the integration of intelligence.[32] It has indirectly led the Agency to misprize a potential consumer market consisting of personnel not cleared for compartmented information.

The present costs of compartmentation in confusion, wasted manpower, less meaningful intelligence, and enhanced risk of intelligence failure could be ameliorated, if not eliminated. As steps in this direction, a series of recommendations are set forth below. They are discussed under

TOP SECRET
Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6
HANDLE VIA TALENT-KEYHOLE-COMINT CONTROL CHANNELS

Next 7 Page(s) In Document Exempt

Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6

the other problems of compartmentation: the establishment of centralized control; vigorous decontrol of information; and rationalization of the structure of the compartments. Still, some steps could be taken to improve the present system and obtain a more holistic intelligence product. Extension of Recommendation 1 (a central repository for information on access approvals) and Recommendation 2 (A Center for Compartmented Information) to the Intelligence Community would be helpful.

The DCI Committee structure is largely a reflection of the divisions attendant upon compartmentation. The NIO system was established to fill the gaps left by the committees. The geographic makeup of the DDO and the predominantly functional one in the DDI and DDS&T hamper coordination among these directorates. And within the latter directorates, there has been a "fragmentation of analytic responsibility." "Because of the many academic disciplines involved, the analysis of weapons systems has been broken into pieces and distributed among the analytic branches in several offices."[40] The recent DDI/DDS&T reorganizations were certainly designed in part to overcome these fragmenting tendencies, but they persist and are reinforced by the operation of the compartments.

Next 4 Page(s) In Document Exempt

Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6

FOOTNOTES

1. Section 9 covers "Special Departmental Arrangements." It states that "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."

25X1A

3. Roberta Wohlstetter. Pearl Harbor, Warning and Decision. Stanford University Press, 1962, p. 174.

4. An article by Peter Szanton and Graham Allison entitled "Intelligence: Seizing the Opportunity" gave this description of the NRO: "National Reconnaissance Office. The largest agency in terms of budget is the National Reconnaissance Office (NRO) also lodged in Defense. The NRO operates the numerous 'overhead' (principally satellite) reconnaissance programs for the community, working largely through the U.S. Air Force. Its products are medium-resolution photographs of wide areas and high resolution pictures of selected points; these are useful to economic analysts and essential to those concerned with military and arms control issues. The NRO is subordinate to the DCI and a deputy secretary of defense." Foreign Policy. First quarter 1976, p. 187. Note: The NRO considers this information "classified and compartmented."

Next 4 Page(s) In Document Exempt

Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6

25X1A
25X1A

48. [redacted], op. cit., p. 4. In an annex to this study [redacted] observes that "the idea of a single compartmentation system is already pretty far along. We have a USIB policy on physical security requirements to protect any compartmented information, a DCID 1/16 on common standards to protect any compartmented material stored or processed on computers, a courier system to handle any compartmented material, and a pretty common understanding of how to log and mark compartmented materials."

Top Secret

[redacted]

Top Secret

Next 1 Page(s) In Document Exempt

Approved For Release 2002/01/08 : CIA-RDP83B00823R000900180001-6