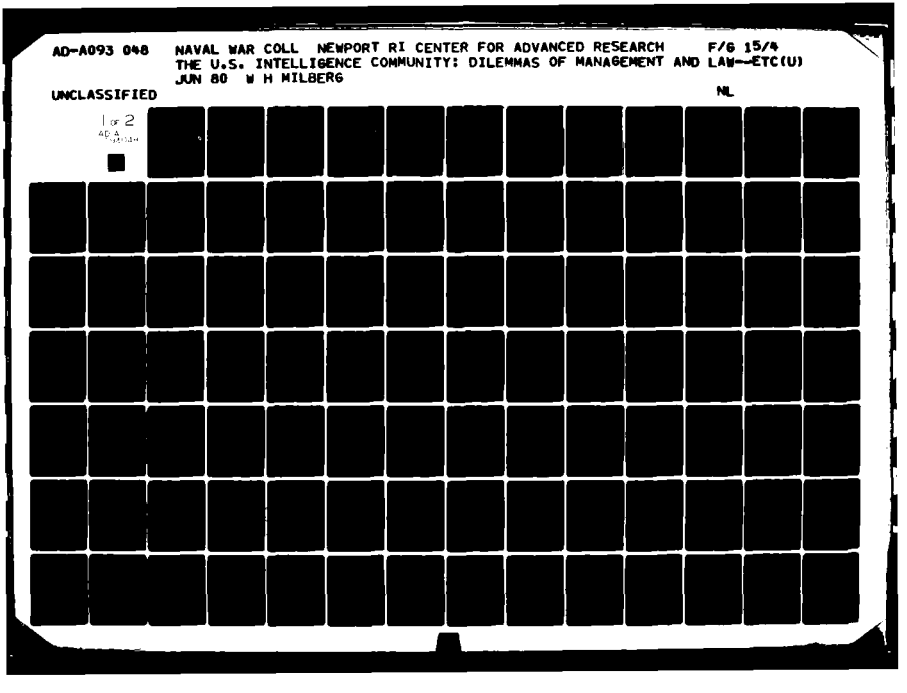
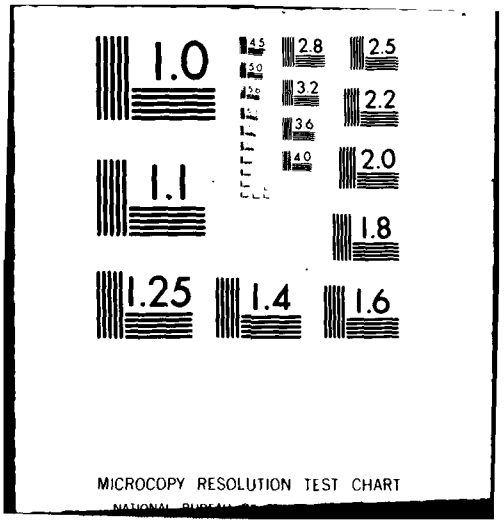
AD-A093 048 NAVAL WAR COLL NEWPORT RI CENTER FOR ADVANCED RESEARCH F/G 15/4
THE U.S. INTELLIGENCE COMMUNITY: DILEMMAS OF MANAGEMENT AND LAW--ETC(U)
JUN 80 W H MILBERG

UNCLASSIFIED NL




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
MICROCOPY RESOLUTION TEST CHART

THE UNITED STATES NAVAL WAR COLLEGE

PUBLISHED BY

THE NAVAL WAR COLLEGE

CENTER FOR ADVANCED RESEARCH

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A093 048
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE *(and Subtitle)* (6) The U.S. Intelligence Community: Dilemmas of Management and Law	5. TYPE OF REPORT & PERIOD COVERED (9) Final rpt
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) (10) MILBERG, WARREN H. ~~MCCOY, CONF~~	8. CONTRACT OR GRANT NUMBER(s) (12) 138
9. PERFORMING ORGANIZATION NAME AND ADDRESS Center for Advanced Research Naval War College, Newport, RI 02840	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Same	12. REPORT DATE (11) Jun[redacted]80
	13. NUMBER OF PAGES 107 + Appendices
14. MONITORING AGENCY NAME & ADDRESS *(if different from Controlling Office)*	15. SECURITY CLASS. *(of this report)* UNCLASS
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

A- Unlimited

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

A - Unlimited

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

Hughes-Ryan Ammendment	Freedom of Information Act
Intelligence community	Classification System
Intelligence management	Leaks
Intelligence oversight	Espionage
Intelligence charters	Graymail

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

This study examines the U.S. Intelligence Community and focuses on the many obstacles which threaten to impede the production of intelligence today. Chief among the concerns discussed are the organizational peculiarities which affect the Intelligence Community as well as such external factors, the unauthorized disclosure or intelligence sources and methods through leaking and espionage. The dilemmas which arise in invesitgating unauthorized disclosures →next page

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

JC12

41026 ×

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

together with a number of legal issues associated with the protection of classified information, are also presented.

THE U.S. INTELLIGENCE COMMUNITY:
DILEMMAS OF MANAGEMENT AND LAW

BY

WARREN H. MILBERG
LTCOL, U.S. AIR FORCE

JUNE 1980

EXECUTIVE SUMMARY

The focus of this study is on the U.S. Intelligence Community -- a term understood by few, but affecting us all in our personal and professional lives. The underlying premise of the study is that due to increasingly scarce resources, and the competition for them engendered by the federal budgetary process, U.S. intelligence products will become an even more important politico-military force multiplier in the coming years. The internal and external factors which now threaten to diminish the U.S. Intelligence Community's ability to continue to provide the President, the Cabinet, the National Security Council, military commanders, and all users of intelligence products with timely, accurate, and useful data concerning the foreign environment are explored in order to add to the public debate about an issue of critical import.

Chief among the problems now facing the Intelligence Community are its organization and management. The Intelligence Community is composed of twelve or more relatively independent agencies, departments, and elements in a loose confederation under the general guidance of the Director of Central Intelligence (DCI). The DCI is at once the senior intelligence advisor to the President and to the National Security Council, the executive head of the Central Intelligence Agency, and the leader and spokesman for the Intelligence Community. Primarily due to limitations on the DCI's

power and authority -- and the unwillingness of the Congress and the American public -- to create a truly effective central intelligence system in the United States, the DCI must manage the resources of this community of disparate activities as a less-then-equal player in the political power structure. The DCI, for example, is not a cabinet member, as are many of the other individuals who "own" significant parts of the Intelligence Community structure, and the overwhelming majority of the U.S. intelligence budget resides in the budgets of larger organizations beyond the DCI's direct control. Further complicating the problem of management and the production of intelligence analyses is the fact that many of the authorities governing intelligence roles and missions are either duplicative in some areas or vague in others. While the DCI may be responsible for "national" intelligence in support of overarching needs of the government, other officials retain operational or budgetary control over "departmental" intelligence resources. Considering the fact that many of the sources of both "national" and "departmental" intelligence (as well as "tactical") are often the same, the DCI enjoys few strong management mechanisms in terms of setting intelligence priorities or directing the use of Intelligence Community resources. Many of the mechanisms now in place consist of a variety of committees, boards, and centers which came about as a result of the latest in a long list of reorganizations of the Intelligence Community. It is hard to see how

this latest reorganization has improved on the DCI's ability -- indeed, the ability of the entire Intelligence Community -- to do the singularly unique job of providing intelligence products in a timely and useful way.

The role of Congress is also explored, primarily from the standpoint of the select committees which came into being after the sensational disclosures of intelligence abuses of power in recent years. These committees have taken an active role in the "oversight" of intelligence activities by becoming involved in intelligence resource allocation issues and their attempts to charter legally an Intelligence Community which, with one minor exception, has continued to operate in a legal vacuum. Legislative charters for the Intelligence Community are a highly charged emotional issue and, due to political realities and day-to-day international tensions, most of these attempts have foundered. Yet closely associated with ill-fated attempts to charter the Intelligence Community are the concurrent attempts to provide legislative remedies for the nagging problem of protecting intelligence sources and methods from unauthorized disclosure.

The ways in which intelligence sources and methods are threatened -- and the analyzed products produced from them as well -- are as varied as are the uses of intelligence. In order to be useful, intelligence must provide information that is not available elsewhere and that information must be made available to a multitude of policymakers and other

consumers at all levels of command and organization. This combination of useful information and wide dissemination has made intelligence products extremely vulnerable to the ever-increasing phenomenon of leaking by officials in and out of government. The study explores this phenomenon to some extent and identifies the 1974 Hughes-Ryan Amendment to the Foreign Assistance Act, the Freedom of Information Act and the government-wide and much abused classification system as unwitting accomplices which have added to the real and imagined problems of keeping secrets secret in America.

The study concludes with a final chapter on how the problem of unauthorized disclosures are investigated and the dilemmas which arise in the courtroom and elsewhere when such cases are brought to trial. The FBI, for example, often refuses to investigate instances of leaking, primarily due to the fact that to do so would mean that they would have few resources left to do anything else. In the rare cases when leaks are investigated, the Intelligence Community must often agree to declassify the information in question first. The dilemma then becomes one of deciding how much more sensitive intelligence information must then be made public in order to protect the sources and methods of the nation's secrets. In the few cases which actually come to trial, additional problems soon arise in that the government may be subject to "graymail" when a defendant uses federal discovery procedures in order to introduce more classified information into open

court. The government has often sought a dismissal of the case at this point rather than run the risk of further damaging "national security."

Finally, the Espionage Laws are examined briefly in order to highlight and illuminate the fact that these anachronistic legal mechanisms provide little, if any, relief to an Intelligence Community which suffers from the preception, if not the reality, of no longer being able to protect its sources and methods from unauthorized disclosured. In the wake of this legal void, a number of administrative remedies have been devised and implemented to stem the tide of leaks, yet many of these measures either apply to only a small fraction of the community of potential leakers or they create yet other dilemmas in an open society which has been historically wary of secrecy.

The study ends on the somewhat positive note that through all the organizational and legal permutations and combinations which have affected the Intelligence Community, intelligence products continue to be produced and disseminated to the people who must have them. While the obstacles in the path of continued intelligence production are numerous and certainly decrease the efficiency of the Intelligence Community, most of the proposed solutions could, in fact, create yet other dilemmas. It may be that living with these obstacles and only attempting change at the margin must be a "cost" which the Intelligence Community will have to bear as it goes about the critically important business of providing the eyes and ears of the government abroad.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

The importance of timely, accurate, and pertinent foreign intelligence cannot be underestimated. Historical examples abound wherein nations either failed to recognize external threats to their security or neglected to establish a streamlined organizational mechanism for determining them in the first place. Intelligence collected, analyzed and disseminated by the ubiquitous yet arcane U.S. Intelligence Community - a term understood by few, but affecting us all - will become a more critical cog in the foreign policy development and implementation processes in the coming years. This is predicated on the fact that intelligence will be increasingly relied upon as a politico-military force multiplier as the competition for scarce budget resources becomes keener. Yet the possibility exists that the President, the Cabinet, the National Security Council, military leaders, and field commanders - all consumers and users of intelligence products - may not continue to have an assured flow of this vital national resource due to organizational and legal peculiarities now affecting the U.S. Intelligence Community.

Intelligence is produced by the twelve or more acitivites which currently comprise the Intelligence Community, a loose confederation headed by the Director of Central Intelligence (DCI). The DCI is at once the senior intelligence official

of the nation, the titular leader and spokesman for the intelligence community, and the executive head of the Central Intelligence Agency (CIA). Over the years since the enactment of the National Security Act of 1947 and the Central Intelligence Agency Act of 1949, successive DCIs have regarded and discharged these responsibilities in different ways. For the most part, DCIs have tended to focus attention primarily on the day-to-day management of the CIA leaving the management of the larger Intelligence Community to the heads of the agencies and activities concerned. This may have come about for a variety of reasons, chief among them being the inherent difficulties any DCI would face in attempting to orchestrate the efforts of governmental activities without the benefit of line - hire and fire - control. Yet each new DCI (there have been five in the past seven years) has directed more and more effort toward managing the Intelligence Community, a community which extends far beyond the organizational limits of the CIA.

Like most elements of the federal government, the Intelligence Community has grown larger and larger; growth which has further complicated and compounded the DCI's problems of insuring that the aforementioned consumers and users of intelligence products continue to receive the best possible intelligence support. Not only has the Intelligence Community grown over the years, but it has also changed in structure and composition as well. Each attempt to streamline the

Intelligence Community has exacted a price which can best be summarized as adding to the DCIs ability to control it in some areas while concurrently clouding the issue of roles and missions. In addition to the internal machinations of the Executive Branch to organize an effective intelligence structure, the Legislative Branch has also become an active participant in the process.

For the first time in our history, two committees in Congress have been permanently established to "oversee" the nation's intelligence apparatus. Congress is not only deeply involved in the budget allocation processes of the Intelligence Community, it has also become an important consumer and critic of its products. The ability of the DCI to satisfy the many and varied needs of its consumers and constituents is further compounded by the myriad laws, executive orders and administrative regulations which purport to govern the Intelligence Community.

Although the DCI is charged by law for the protection of intelligence sources and methods, leaking and other forms of unauthorized disclosure have added to his problems in that few statutes adequately allow for the prosecution of persons who decide to compromise sensitive materials. The DCI and the Intelligence Community, however, are not entirely without recourse in their battle to stem what appears to be an ever-increasing tide of unauthorized disclosures. Certain attempts to allow the DCI to carry out his statutory responsibility for

the protection of intelligence sources and methods have worked quite well; others have often resulted in the Intelligence Community looking foolish, incompetent, or vindictive. The heart of the controversy is how to balance the public's right to be informed about important national and international events while concurrently insuring that the minimum level of secrecy and security needed to conduct intelligence activities is maintained.

The purpose of this study is to illuminate some of the complex organizational and legal issues surrounding this nation's continued ability to produce intelligence products. While all three branches of government have certain responsibilities which at least peripherally relate to the production of intelligence analyses, discussion centers on how management is accomplished in the Executive and Legislative Branches - and whether such management helps, hinders, or is otherwise neutral in assisting the Intelligence Community with its singularly unique task of providing "adequate" analyses to the people and organizations which must have them. As will be seen later on, the judiciary affects the production of intelligence products through the interpretation and application of certain laws. But as this paper is completed in the Spring of 1980, few required laws affecting the business of intelligence most notably laws relating to clear charters for the Intelligence Community and the safeguarding of the sources and methods upon which intelligence analyses are based, are on the books.

Indeed, most of the required laws, in the opinion of the author, are still in the formulation and negotiation stage and may never be enacted.

In attempting to examine the multitude of organizational and legal issues surrounding the nation's ability to continue to obtain and use inteligence products, it has become apparent that many of these issues could, in and of themselves, become the basis for individual case studies. Such an approach was rejected, perhaps at the cost of a deeper and more thorough-going analysis of certain of these problems, in order to present a fuller picture of the magnitude of the problems now facing the U.S. Intelligence Community. This macrocosmic approach is intended to inform the non-intelligence community of individuals and organizations who use, indeed, depend on, intelligence products in their daily lives, of just a few of the myriad problems of intelligence management in our open and democratic society and to thus add to the public debate on a subject of critical importance. It is concurrently hoped that this paper will also highlight and illuminate problems which may spark further study by intelligence professionals, in the Executive as well as Legislative Branches, which, in the end, will result in improving the likelihood that the U.S. Intelligence Community can continue to provide a unique service to the nation.

CHAPTER II

THE U.S. INTELLIGENCE COMMUNITY

Interest in Intelligence

Within the United States, and perhaps elsewhere, the term "intelligence" carries with it certain emotional overtones. To those caught up in the growing fear that the nation is inexorably moving to the conservative right, concern centers on the amount of power the federal government has aggregated unto itself - and what that may portend in terms of civil liberties and abuses of intelligence power.[1] At the other end of the poltiical spectrum, attention is focused on the proliferation of rules, regulations, and laws which appear to so threaten and restrict intelligence activities that they will become hamstrung and ineffective.[2] The debate tends to obscure a real issue for the majority of citizens, in and out of government, who fall somewhere in between: how well do U.S. intelligence activities serve the needs of the nation?

Considering the size, nature, and function of the federal bureaucracy, perhaps nowhere is there more truth in the cliche that knowledge is power than as it is applied to the executive, legislative, and judicial branches of government.[3] If knowledge is power, it must share the limelight with money: who gets a piece of the half-trillion dollar federal budget, and how they spend it, is a primary activity in official Washington. In this system, the role played by

the U.S. Intelligence Community is critical: they often provide, deny, interpret, and misinterpret information (i.e., knowledge) concerning the international arena which is then used as an input into the foreign policy development and implementation processes of the U.S. government.[4] And occasionally seemingly egregious errors directly or indirectly result in turmoil throughout the intelligence bureaucracy.

On November 11, 1978, for example, President Carter sent a letter to then Secretary of State Cyrus Vance, the Assistant for National Security Affairs Zbigniew Brzezinski, and to Director of Central Intelligence (DCI) Stansfield Turner, that stated that he was ". . . dissatisfied with the quality of political intelligence."[5] The President's letter, of course, stemmed from the revolution which had just occurred in Iran, most notably the Intelligence Community's so-called failure to predict the strength and resolve of the Islamic nationalists opposed to the continued rule of Shah Mohammed Reza Pahlavi. Regardless of whether there was an "intelligence failure,"[6] the President's letter necessitated, inter alia, yet another review of the organization, mission, and functions of the U.S. Intelligence Community. But failures notwithstanding, interest in intelligence activities has been charachteristic of our society for some time. Former DCI William E. Colby states why:

> Rock stars, international jetsetters, and even such subjects as environment, future food shortages, and energy seem to rise to top billing and then fall as public attention wanes and turns to other things.

> But the Central Intelligence Agency is a perennial, from the Bay of Pigs in 1961 through the national student association [sic] exposure in 1967, Watergate in 1972, and the frenzy of 1975 about domestic activities, assassination plots, coups and secret wars.
>
> * * * * * * * * * * *
>
> Spy novels have attracted readers for decades. The atmosphere of intrigue fascinates with its mixture of hidden influence and ruthless power, and seeing in the open what was hidden so long seizes attention.[7]

Mr. Colby correctly equates public interest in intelligence activities with the Central Intelligence Agency (CIA), rather than with the Intelligence Community. And therein lies the first problem: intelligence activity has come to be synonomous with the CIA in the public mind and, to some extent, in the private view as well. Yet there are at least eleven other departments, agencies, elements which participate in the intelligence process in one way or another and are a part of the Intelligence Community. Further compounding the problem of understanding - and managing - the Intelligence Community is the fact that although its antecedents can be traced back to the World War II Office of Strategic Services, to the post-war Central Intelligence Group, and to the intelligence components of the Army, Navy, and State Department, it has undergone rather continuous change and reorganization since those times.[8] In its current configuration, the Intelligence Community is just a little over two years old and, in terms of management, oversight, and administration, nothing even remotely similar to it exists in the federal bureaucracy. Whether or

not recent events result in another reorganization, it seems useful to explain what now exists, how intelligence analyses are managed considering the de facto and de jure forces extant in the bureaucratic environment, and to suggest factors which deserve consideration in the future.

A prerequisite to understanding the Intelligence Community - and the types of analytical products it produces - is an understanding of the "intelligence cycle."[9] The Joint Chiefs of Staff define the "intelligence cycle" as the "steps by which information is assembled, converted into intelligence, and made available to users."[10] The importance of definitions cannot be underestimated in the federal bureaucracy in general, and in the Intelligence Community specifically: they are the critical inputs used to determine which agency performs what mission, and hence can lay claim to people, programs, and other resources through the budgetary process.[11]

Intelligence Production Responsibilities and Anomalies

Over the years the author has had the opportunity to make numerous presentations to public and private groups on various aspects of the intelligence profession. The audiences have been varied, ranging from mid-career civilian and military officers attending the Defense Intelligence School to graduate students majoring in international security studies. Although the level of knowledge about the Intelligence Community can probably be described as moderate to very low, invariably a single factor became apparent during the presentations: in

all cases a significant amount of erroneous preconception or misperception was evident. Whan asked what the "Intelligence Community" included, most audiences responded with CIA, the Federal Bureau of Investigation, and perhaps even the Defense Intelligence Agency. Some of the more sophisticated groups occassionally added the National Security Agency (without knowing that it was a part of the Department of Defense). In no case was the entire composition of the Intelligence Community mentioned. This may not seem surprising considering the real or imagined cloak of secrecy which has surrounded the intelligence process in America over the years, yet numerous unclassified sources of information on this subject have been, and continue to be, readily available.[12] Also, as David Wise sarcastically states, the term "Intelligence Community" is viewed as a "homey phrase that conjures up visions of neatly trimmed lawns and outdoor barbecues."[13] It is far from that. In its most formal sense, the Intelligence Community consists of the following:

<u>Independent Agency</u>

The Central Intelligence Agency

<u>Departmental Intelligence Elements</u> (non-DOD)

Federal Bureau of Investigation
Department of the Treasury
Drug Enforcement Agency
Department of Energy
Department of State

Department of Defense (DOD) Intelligence Elements

Defense Intelligence Agency
National Security Agency
Army Intelligence
Navy Intelligence (including Marine Corps)
Air Force Intelligence
The offices within the DOD for the collection of specialized national foreign intelligence through reconnaissance programs

Staff Offices of the Director of Central Intelligence

Intelligence Community Staff[14]

The purpose of listing these components of the Intelligence Community does not stem from some subliminal urge to set the record straight, but rather to highlight and illuminate the diverse nature of this complex, perhaps even labyrinthine, bureaucratic beast. No one need be a student of government or even organizational behavior to begin to comprehend how such a "community" consisting of relatively independent agencies having literally thousands of employees, on the one hand, to tiny parts of other large departments, with just a few individuals engaged in the intelligence process, on the other hand, will have immense and inherent management problems from the outset.

More important than numbers of employees is the fact that some intelligence agencies, departments and activities have more or less total responsibility for the full panoply of topics on which intelligence must be produced, while other components of this loose confederation have significantly lesser responsibilities.

The CIA, for example, has the responsibility to "produce and disseminate foreign intelligence relating to the national security, including foreign political, economic, scientific, technical, military, geographic and sociological intelligence to meet the needs of the President, the NSC, and other elements of the United States Government."[15] The Department of State is charged with production and dissemination of foreign intelligence having to do with U.S. foreign policy which the Secretary needs to carry out his responsibilities, while the Department of the Treasury must produce foreign intelligence relating to economic policy that the Secretary of that department requires in the performance of his statutory duties.[16]

The Secretary of Defense, on the othr hand, is responsible for the production of foreign military and military-related intelligence information which includes scientific, technical, political, geographic, and economic data that he needs to do his job.[17] And finally, the Director of the FBI "produces and disseminates foreign intelligence, counter-intelligence, and counterintelligence studies and reports."[18]

The point of the foregoing sample of intelligence production responsibilites, as abstruse as it may seem, is that the assignment of production tasks may be construed as either positive or negative depending on your organizational interests and frame of reference. The number of competing centers of intelligence analysis extent in the Intelligence Community should insure objectively different points of view; yet they

also compound the problems of management. That job falls squarely on the shoulders of the Director of Central Intelligence who is, afterall, the nation's senior intelligence analyst.[19] But before examining the mechanisms available to him to oversee the production of intelligence analyses throughout the government, it is necessary to briefly return to definitions, this time to three generic types of intelligence: national, departmental, and tactical.

National, Departmental, and Tactical Intelligence

Depending on the context of usage, the term "intelligence" may mean (a) information, that is, some form of assessed data; (b) the assets used to collect and evaluate that data: and (c) the process by which data is collected and evaluated. Yet any definition of intelligence as an assessed product must be considered in terms of how the ultimate recipient - the policymaker - uses it. As can be seen from the summary of some of the analytical tasks assigned to the various components of the Intelligence Community, the uses of their individual or corporate analyses differ substantially.

"National" intelligence, for example, can be construed to mean those analytical products which cover broad aspects of national policy to the extent that it transcends the needs and exclusive competence of departments and agencies to carry out their overall missions. "Departmental" intelligence, as the name implies, is that analytical data required by a department or agency to accomplish its assigned mission.

"Tactical" intelligence concerns data about the strength, disposition, composition, and capabilities or military forces - to include such planning information as weather and geography - that military commanders require to plan for, and conduct, military operations.[20] These definitions are simplified, of course, but they underscore the problem of overlap and duplication that exists within and among intelligence analytical centers. Just as a reconnaissance photograph of a column of Soviet tanks moving across the German Democratic Republic would be of obvious interest to U.S. military commanders in Europe, so to would it be of interest to various officials at the Department of Defense level, to include the Joint Chiefs of Staff. It is also not hard to conceive of scenarios where this same photograph would attract the attention of the National Security Council - and perhaps even that of the President.

The fact that the means used to collect and produce intelligence in order to satisfy national, departmental, and tactical intelligence requirements are often the same further complicates the problem of managing intelligence analyses. The President has given the DCI "full responsibility for production and dissemination of national foreign intelligence and . . . (the) authority to levy analytical tasks on departmental production organizations."[21] But yet at the same time, the Secretary of Defense, in addition to satisfying his own departmental intelligence requirements, must "conduct programs

and missions necessary to fulfill national and tactical intelligence programs," as well.[22] One might logically conclude that the all-encompassing nature of the DCI's responsibility for national intelligence would also include responsibility for managing departmental and tactical intelligence production. But that is not the case. Management, in this sense, is not line authority over people and assets, but rather the responsbility to insure that the hierarchial needs of all intelligence users are satisfied. The Department of Defense, concerned that the DCI may not be sensitive enough to this "national-tactical" interface, created yet another category of intelligence activity known as "intelligence-related activities."[23]

Intelligence-Related Activities. Intelligence-related activites are defined by the Department of Defense as follows:

> . . .those activities outside the Consolidated Defense Intelligence Program which: respond to operational commander's tasking for time-sensitive information on foreign enemies; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities.[24]

As such, intelligence-related activities again complicate the DCI's management responsibilities for the production of national intelligence in that these assets may not be responsive to him if the collection and analytic tasks levied on them are not primarily responsive to the needs of military commanders at the same time. One can only rhetorically wonder

if the time-sharing of intelligence assets across the full spectrum of national, departmental, and tactical - to include intelligence-related - consumer needs is the best, or most efficient, system that can be devised.

CHAPTER III

PROBLEMS OF INTELLIGENCE MANAGEMENT AND ORGANIZATION

It is important to again stress that while the term "management" includes all facets of intelligence activity supervision, emphasis is placed herein only on the factors which contribute to, or retard, the production of intelligence analyses. For this reason the functions of the President's Intelligence Oversight Board, Intelligence Community Inspectors General and General Counsels, as well as the Attorney General, all of which have significant responsibilities for questions concerning the legality of propriety of intelligence activities, will only be peripherally treated in later sections of this paper. These mechanisms came into being, or were strengthened, primarily as a result of the abuses of power attributed to the Intelligence Community in the past; however, they have few, if any, direct responsibilities for that aspect of intelligence activity having perhaps the greatest potential for future abuse: the quality of intelligence analysis. This comment is based on the observation that ". . . the adequacy of intelligence (has) narrowed American policy choices."[1] In speaking of the importance of knowing the dangers extant in the international system, Senator Malcolm Wallop, a member of the Senate Select Committee on Intelligence, pointedly draws the following analogy between the quality of intelligence analyses and abuses: "What intelligence abuse could be greater than the

failure to warn the American people . . . ?"[2] Of all the means and mechanisms used to manage the production of intelligence, the President is by far the most important and influential.

The Role of the President

Although not usually considered in many discussions of the Intelligence Community, the President, as the chief executive, must be considered to be at the top of the structure. The President heads the National Security Council which, *inter alia*, "is the highest Executive Branch entity that provides review of, guidance for, and direction of all national foreign intelligence and counterintelligence activities."[3] Moreover, the President nominates the DCI and is largely responsible for determining the mission, organization, and fuctions of the Intelligence Community.[4] And considering that the ultimate function of the Intelligence Community, as a service and support activity of government, is the satisfaction of information needs, then the needs of the President, it may be argued, probably take precedence over all others in a *de facto*, if not *de jure*, sense. The fact that the products of the Intelligence Community will be directly influenced by the perception - if not the statement - of what the President's needs may be necessitates an explanation of how these needs, as well as those of lesser users of intelligence products, are articulated and acted upon. Within the National Security Council, the Policy Review Committee (PRC) plays a critical role in this regard.

The Policy Review Committee

When meeting on intelligence matters, the NSC Policy Review Committee is chaired by the DCI and consists of the following members: the Vice President; the Secretaries of State, Defense, and Treasury; the President's Assistant for National Security Affairs; and the Chairman of the Joint Chiefs of Staff. Other agency heads or individuals, such as the Attorney General or the Director, Office of Management and Budget, may be invited to specific meetings depending on the subject matter to be discussed. This committee plays a central role in the management of intelligence analyses as it: sets national foreign intelligence requirements and priorities; reviews the intelligence budget in terms of adequacy in meeting the foregoing requirments and priorities; and performs a quality control function by evaluating resultant intelligence products.[5]

Requirements and Priorities. The importance of establishing requirements and priorities cannot be underestimated: they determine, at least in theory, the focus of Intelligence Community efforts - and thus play curcial roles in the formulation of the national foreign intelligence program budget - the means by which information needs are transformed into plans, programs, and human activity.[6]

The immensity and difficulty of this task becomes somewhat clearer by understanding the fact that since the

the foreign policy of the United States is global in nature, so too are the supporting analytical tasks assigned to the Intelligence Community. At the most simplistic level, the reader is encouraged to think about this problem in terms of a basic matrix listing all of the countries of the world across the horizontal axis of the matrix, while the vertical axis consists of the infinite variety of problem sets and subsets representing all of the various types of political, military, economic, scientific, and sociological subjects which could conceivably be of interest to the users of intelligence at all levels of government organization. The foregoing should not be construed to portray accurately the process used by the PRC to set Intelligence Community requirements and priorities, but to only underscore the magnitude of the problem at hand.

The concept of assigning the highest level consumers of intelligence analyses - the members of the PRC - the task of determining Intelligence Community requirements and priorities is new, having only been initiated with the Carter Administration's reorganization of the Intelligence Community in January 1978. Prior to that time, the Community generally established the focus of its efforts internally. Intelligence professionals, thought to be more familiar with the capabilities and limitations of intelligence programs and systems, had traditionally disdained the concept of allowing "outsiders" to set the priorities which would guide, control, and oversee

intelligence production. President Carter changed that long-standing tradition by charging his PRC with the task - and gave them budgetary control to insure that their responsibility also had the requisite authority to make it work. But has anything really changed?

As can be seen from the PRC's membership, next to the President they are the nation's most important users of intelligence analyses - they are the policymatkers - certainly they should have a voice in determining what intelligence analyses they must have. But priorities do not automatically result in "good" intelligence products. And judging from the President's letter quoted earlier, as well from recent events in Afghanistan, the highest level intelligence consumers do not seem to have established a better track record than the professional intelligence officers formerly discharging this responsibility. It then would seem that in order to make this responsibility more efficient, the PRC members must become more intimately familiar with the capabilities and limitations of Intelligence Community programs, and they must also become more aware of how their intelligence requirements and priorities are translated into actual activities designed to collect raw, unevaluated data, how such programs are implemented, and how the resultant products are evaluated. Considering the magnitude of the other responsibilities of the PRC members, whether or not they have the time, inclincation, or ability to absorb such knowledge is problematical at best.

Chief among the other concerns at this level of intelligence management are the unknowns that exist in attempting to equate and relate intelligence requirements and priorities to the intelligence budget; and the methodology used to determine and evaluate the "quality" of intelligence products before, rather than after, an "intelligence failure." Perhaps most importantly, the DCI may be at an inherent disadvantage when chairing this committee in that he is not a cabinet member nor a statutory member of the NSC, as are most of the other participants. This situation is exacerbated by the probability that perhaps as much as three-fourths of the intelligence budget is included in Department of Defense programs - and at least the "intelligence-related" items are beyond the management control of the DCI.[7]

The National Intelligence Tasking Center

Recognizing the predominant role of collection in the intelligence process, the President created the National Intelligence Tasking Center (NITC), under the control and direction of the DCI and gave it the responsibility to translate the requirements and priorities developed by the PRC into specific collection objectives and targets. The NITC was also given the responsibility of assigning these objectives and targets to the organizations which control national intelligence collection systems needed to satisfy them.[8] The NITC, as a collection management activity, can then be seen as impacting on the production of intelligence analyses in

one of the most critical ways of all: it is charged with controlling and directing the analysts' sources of raw material. The intelligence analyst - the principal individual responsible for meeting the needs of both high and low level users of intelligence - can then be viewed from the perspective of being rather heavily, if not totally, dependent on how well the collector interprets consumer needs, on how well he successfully tasks the systems needed to produce unevaluated data, and on how well he supplies it to the analyst. And this situation obtains before the analyst even begins to think about drawing conclusions about world events. If this system of consumer/collector/analyst interaction operated as conceived in the abstract, perhaps there would be little cause for concern. But among other things, Congress approved only about half of the personnel required to manage this critical cog in the intelligence process and, not unexpectedly, the NITC has had concomitant bureaucratic problems from the very beginning. Certainly the quality of intelligence analysis has not improved in the process.[9] Although not a formal part of the President's January 1978 reorganization of the Intelligence Community, the National Foreign Assessment Center (NFAC) must also be considered a central actor in the lineup of Executive Branch intelligence management mechanisms.

The National Foreign Assessment Center

As stated earlier, the DCI has near total responsibility for the production of national foreign intelligence. This

responsibility transcends the analytical activities undertaken by the CIA: it applies to the entire spectrum of analytical capabilities throughout the Intelligence Community. To discharge this responsibility, the DCI created the National Foreign Assessment Center to organize, manage, and oversee the production of national intelligence.[11]

In essence, the National Foreign Assessment Center represents a consolidation of the extant National Intelligence Officer structure with the production elements within the CIA. Interestingly, the NFAC is concerned primarily with producing estimative, as opposed to descriptive, national intelligence products. The director of this Center is also responsible, through the DCI, for liaison with the NSC, the Cabinet, the Congress, the entire Executive Branch, and even the public, on matters of substantive national foreign intelligence.[12] But at least in a de jure sense, the NFAC would not seem to have any responsibility for an input into the development of intelligence requirements and priorities, nor the control and tasking of the means and mechanisms used to collect the raw data needed to produce intelligence products. And considering bureaucratic behavior and institutional proclivities, as well as how various components within the Intelligence Community view their responsibilities to contribute to their own departmental intelligence needs, the potential for problems in taksing non-CIA analytical centers in support of national intelligence suggests that the whole concept of a national

assessment center requires further thought and consideration. In this regard, the National Foreign Intelligence Board (NFIB) can be considered yet another mechanism which both helps and hinders the production of national intelligence.

The National Foreign Intelligence Board

The National Foreign Intelligence Board, composed of the senior representatives of the Intelligence Community, serves the DCI in an advisory capacity relative to the production of national intelligence, the level and content of the intelligence budget, and on other matters of common concern.[13] In effect, the NFIB is the Intelligence Community's corporate board of directors - or, more appropriately, its board of advisors as it has no formal Community power or line authority. It is here that differences between Intelligence Community components concerning judgment and opinion contained in national intelligence products are raised and, hopefully, resolved. Although this Board can only be as effective as the DCI will allow it to, the DCI is specifically responsible for ensuring "that diverse points of view are considered fully and that differences in judgment within the Intelligence Community are brought to the attention of policymakers."[14]

Until a few years ago, dissenting opinion was contained in footnotes to the analytical text of national intelligence estimates that came before the NFIB for consideration. Like most bureaucratic organizations, the NFIB strove for common consensus in its estimates in order to portray a unified

opinion to the policymakers for whom the estimates were drawn. Yet senior intelligence officials often viewed the world, and the events which could occur in the international system, through differing organizational prisms. As more and more dissent began to appear in estimates - and it should be pointed out that while some dissent was honestly conceived, other footnotes to the text took on at least the appearance of being drafted in support of institutional rather than national policies - a dramatic change took place: dissenting opinion was included into the text itself.[15] Considering the fact that national intelligence estimates are normally quite lengthy in nature, and that the policymakers who receive them probably have limited time to review them, this change has tended to obscure, if not cloud, the entire estimative process. Whether this system now provides enough visibility to dissenting opinion - thus lending objectivity to the analytical process - is a question which would seem to demand reexamination. In other words, do national intelligence products, in fact, reflect the best analytical evidence available throughout the Intelligence Community and is it provided in the most convenient and readable form? The current DCI, in describing how he carries out his responsibility for the production of national intelligence, says that once a draft analytical product is prepared by the Intelligence Community and submitted to the NFIB for reivew ". . . at that point the <u>one-man system comes in</u>, because I decide, I sign

for it, I vouch for it. . . ."[16] (emphasis added). So it would seem that while the DCI continues to meet the intent of his charter to provide the policymaking community with both agreed-to estimates as well as dissenting opinion, whether the spirit of that charter is being met becomes a highly controversial and sensitive question. The final element of Executive Branch management mechanisms involved in the function of intelligence analysis is the relatively new Review Panel.

The Review Panel

The concept of having non-intelligence experts, with theoretically no policy preferences to support nor organizational ties to color their objectivity, review the products of the Intelligence Community, is certainly not new. Various permutations and combinations have been attempted over the years and most of these efforts have not noticeably or significantly aided the Intelligence Community discharge its unique and complex tasks. The current Review Panel consists of three individuals with backgrounds in foreign affairs, international relations, and political science.[17] While it seems too early to determine how well this panel, which replaced the now defunct President's Foreign Intelligence Advisory Board, will affect the long term quality of intelligence analyses, it does raise the issue of the need for further quality control efforts from outside the Intelligence Community if for no other reason than logic suggests that a one-man system requires an honest broker.

While it is beyond the scope of this paper to examine all of the attempts to utilize non-intelligence community experts to balance the estimative conclusions of professional intelligence officers, it is somewhat instructive to review briefly the most widely publicized attempt at outside analysis: the so-called "A Team - B Team" experiment in competitive analysis. This experiment brought together a distinguished group of former intelligence professionals, academics, and other individuals with national reputations as experts in Soviet affairs. The purpose of the experiment was to provide this group with exactly the same data that was available to the Intelligence Community in order to estimate Soviet strategic force levels and objectives.[18] Not unexpectedly, the team of outside experts arrived at rather starkly different conclusions than did the Intelligence Community insiders. The point here is not re-analyze the conclusions of either group, but to draw the observation that, at the bottom line, the Intelligence Community, policymakers, and the public profited from the experiment as it added information to the public dialogue about an issue that is still being debated. More specifically and narrowly, it forced the Intelligence Community analysts to rethink their methods and conclusions. It seems useful to look at some of the reasons why the outsiders reached such different conclusions from the insiders. They were, in the opinion of two former "B Team" members:

> . . . free from bureaucratic and institutional factors that tend to reduce conclusions to the low common denominator dictated by an 'agreed intelligence' report, which in the final analysis cannot remain totally insensitive to the framework of Administration policy . . . it was (also) free to address and bring into its product the type of historical, social and political analysis seldom found, at least explicitly, in national itelligence estimates of strategic forces.[19]

Although the "A Team - B Team" experiment did, in fact, result in certain revisions of the estimate prepared by the intelligence professionals, the value of the experiment as a mechanism to improve intelligence products was soon over-shadowed by the plethora of leaks and other unauthorized disclosures which became public as each side sought to justify its positions. The atmosphere of acrimony and recrimination which soon followed has thus diminished the probability of the institutionalization of such experiments in the future - and the Intelligence Community, the policymakers, and the public would all seem to be the losers as a result.[20]

CHAPTER IV

THE CONGRESSIONAL CONNECTION

Over the years, Congressional interest in the Intelligence Community has dramatically changed. Less than 10 years ago a few men in Congress were privy to the innermost workings of the Intelligence Community. Vitenam, Watergate, and the sensational investigations and revelations of the Pike and Church Committees just a few short years ago changed all that.[1] For the first time in the history of the United States, permanent select committees on intelligence have been established in the House and the Senate. The resolutions which established these committees to oversee and manage the activities of the Intelligence Community include specific language relating to the quality of intelligence analyses - and, by extension, Congress has chosen to become interested and responsible for some of the factors which improve or retard the production of these analyses. Although David Wise was referring to covert operations when he said that "the ostrich era is over," his comment applies equally to the fact that a new age has dawned wherein Congress has assumed some of the responsibility with the Executive for insuring that the Intelligence Community is able to produce the kinds of products needed by decisionmakers at all levels.[3] Yet this newly found responsibility is not without its perils, pitfalls, and tensions. William R. Corson describes the situation in the following words:

> The future of American intelligence is beset with uncertainties and several as yet uncontemplated problems. Much more is at stake than the historical battles among the intelligence community members for dominance over one another; rather, it is a battle among the president, the intelligence community, and . . . the Congress over who will actually control the entire intelligence community. This battle - which, as the record shows, has been building for many years - is now upon us.
>
> It is a complex battle whose dimensions have attracted little public attention, but which go to the heart of the question concerning the ability of the intelligence community to produce the kinds and amount of intelligence the president needs to conduct national policy in a coherent and rational manner.[4]

The tone and tenor of Senator Daniel K. Inouye's first annual report to the Senate on the work of the permanent Select Committee on Intelligence amply demonstrates that Congressional interest in intelligence activities need not be confrontational, but could be cooperative if a measure of trust existed between the Congress and the Intelligence Community.[5] Trust is the critical element in this relationship as it implies that Congress can obtain - and protect - the sensitive intelligence materials that it must have not only to oversee intelligence activities, but also to perform its constitutional role of helping to shape the foreign policy of the United States. Senator Brich Bayh, the previous chairman of the Senate Select Committee on Intelligence, has described his committee's role as thus requiring "full access to all information relating to intelligence activities."[6] But the atmosphere of trust and comity that so newly characterizes the relationship between the Congress and the Intelligence Community is, to some extent,

dependent on a number of crucial actions on the part of Congress in the coming months and years. The actions which directly or indirectly affect the continued ability of the Intelligence Community to produce intelligence analyses are described below.

Charters Legislation

As the establishing resolutions of the two intelligence committees of Congress state, the role of Congress is far more than enacting restrictive legislation and castigating the Intelligence Community when "intelligence failures" occur. As described earlier, the Intelligence Community is an organiztional labyrinth with some components having severely overlapping missions and functions. In other cases, responsibility for certain intelligence and intelligence-related activities is obscure or not clearly assigned, but left to the individual components of the Intelligence Community to work out for themselves. The National Security Act of 1947 created the CIA and provided it with something of a "legal" charter. Yet thirty-three years have passed and the role of the CIA has changed in many significant ways. Perhaps more importantly, a large and powerful Intelligence Community has come into being which now includes a dozen or more components, each vying for resources which become scarcer with each budget cycle.[7] With the exception of the Foreign Intelligence Surveillance Act of 1978, the 1974 Hughes-Ryan Amendment to the

Foreign Assistance Act, and the FY 1979-1981 intelligence budget authorization bills, the legislative record of the Congress in dealing with pressing intelligence issues is indeed sparse. This record, says William Corson, ". . . shows a curious thirty-year lag in the agreed to, but never genuinely achieved, central intelligence system."[8]

Recognizing the need for the passage of clear, concise, realistic, and pragmatic legislated charters for all agenices, components, and elements of the Intelligence Community, the Senate Select Committee introduced a bill in the last Congress to totally restructure the Community (the House of Representatives Permanent Select Committee on Intelligence introduced companion legislation, as well).[9] Known as the National Intelligence Act of 1978, this bill was introduced in a variety of forms only to eventually languish and die since the Church Committee finished its investigations of the Intelligence Community in 1976.[10] Although the editors of the Wall Street Journal correctly stated that this bill did not ". . . address the funadmental issues of what intelligence does the U.S. need and how is the U.S. to acquire it," and that ". . . the time spent fine-tuning the bill . . . has permitted more important facts about the nation's intelligence capabilities, or lack thereof" to be better understood, they have failed to understand that clear charters are a first priority and a prerequisite to improving the quality of intelligence analyses.[11] Although this first attempt to lay out a

comprehensive legislative framework for the Intelligence Community did not succeed, Congress continued to grapple with the problem of legal charters, organization and oversight of the Intelligence Community. A number of Intelligence bills have, in fact, been introduced in the current Congress yet as this paper is completed in the Spring of 1980 the likelihood of a passage of any comprehensive measure seems dim at best.[12] The reasons for this Congressional inaction are many and varied, yet in addition to election year politics, the CIA - as well as the rest of the ubiquitous Intelligence Community - has been viewed as hamstrung by the few legislated restraints which affect its operations. This is particularly true in the aftermath of the revolution in Iran and the Soviet invasion of Afghanistan, events which have, inter alia, signaled that the reality, if not the perception, of an Intelligence Community organized and bounded by law, will not be accepted by a public which now chooses to "unshackle" its intelligence arm.[13] The ill-fated story of dead-end attempts to legally charter the U.S. Intelligence Community has another side to it though, and that concerns the various attempts which have been made to include within such charter legislation increased power to protect the extremely sensitive sources, methods and data upon which all intelligence analyses depend.[14]

Sources and Methods. The DCI, being responsible for the production of national foreign intelligence, is concurrently responsible for the protection of sources and methods used by the

Intelligence Community as it goes about the task of converting raw data into analyzed final products.[15] Obviously, if the sources and methods of intelligence production cannot be adequately protected, resultant current analyses will be affected and the efficacy of future analyses will be threatened as well. The ways in which intelligence sources and methods are jeopardized are as varied as are the potential remedies. Leaks by individuals in all branches of the government have become endemic, the ancient art of espionage shows no sign of abatement, the classification system is abused, and the continued ability of the Intelligence Community to produce intelligence is diminished as sources dry up.[16] The Director of Central Intelligence sums up the problem of unauthorized disclosures of sensitive intelligence information this way:

> . . . I have come into the habit of screening the press clips first thing every morning. I almost hold my breath until I know if <u>today's disclosures</u> include some of our sensitive sources of intelligence. (emphasis added)
>
> Sometimes it comes as a leak, sometimes from the forced testimony of one of our officers in court, and sometimes from the subpoena of a document or notes. . . .[17]

But stopping the problem of unauthorized disclosure through legislation (or any other way, for that matter) is not as simple as it might initially appear. The attempted prosecution of leakers and spies under existing statutes has given rise to a whole new set of problems - and new laws - which balance our society's need for openness with workable laws

which protect valid secrets - are now being considered by the Congress.[18] The final chapters review the nature of the problem of maintaining secrecy in a democracy and the dilemmas which arise when current laws or administrative actions are invoked to stem what appears to be an ever-increasing tide of public disclosure of sensitive intelligence data.

CHAPTER V

THE PROBLEM OF KEEPING SECRETS SECRET

The foregoing chapters have briefly considered some of the more visible and important internal organizational roles and missions dilemmas now confronting the Intelligence Community and impeding intelligence analyses. The role of Congress was touched upon from the perspective of past and current efforts to update, amend, or replace those sections of the National Security Act of 1947 that relate to the responsibilities and authorities that continue to affect the Intelligence Community today. The final chapters examine the other side of the intelligence coin: the factors external to the Intelligence Community which may also threaten its ability to produce timely, accurate, and useful intelligence products. These factors are generally subsumed under the overall rubric of protecting intelligence sources and methods and include such phenomena as leaking, the Freedom of Information Act, the Hughes-Ryan Amendment to the 1974 Foreign Assistance Act, and the government-wide classification system.

The Need for Secrecy

Contrary to the prevalent view of many civil libertarians that any amount of secrecy is the antithesis of democracy, the history of the United States is replete with examples of how secrecy -- albeit wisely applied considering the needs of the public to be informed -- may, in fact, be beneficial to

the society. One need only consider the use of the secret ballot on election day, attorney-client and doctor-patient relationships, crop statistics accumulated by the Department of Agriculture, and the privacy of income tax returns in order to appreciate how the concept of secrecy has improved the workings of democracy in America.[1] Just as the need for these "accepted" forms of secrecy is taken for granted in our everyday lives, the need for some minimum degree of secrecy in intelligence activities must also be accepted as a cost associated with maintaining our way of life. In speaking of the importance of intelligence and the maintenance of national security, the Murphy Commission said:

> The maintenance of intelligence capabilities of the highest competence is essential to the national security and to the effective conduct of U.S. foreign policy. The world which American foreign policy seeks to affect is diverse, complex, and rapidly changing. In such a world, policy must be based on detailed understanding of many issues, military, economic, political and scientific, foreign and domestic. . . . much of the most critical information -- especially though not solely, information concerning the military activities and capacities of potential antagonists -- is not openly available.
>
> The responsibility for gathering, evaluating and reporting such information, and for assessing its significance in combination with data openly available, is the primary mission of the U.S. intelligence community. The Commission believes that mission will remain crucial to U.S. security, and to international stability and peace for the foreseeable future.[2]

The ways in which intelligence are collected and analyzed are as varied as are the uses to which it is put. Reduced to basics, the three generic forms of raw intelligence stem from

photographic, signal, and human sources. Once analyzed, finished intelligence products are used by the Department of Defense, for example, to configure and equip the U.S. military force structure; to train and reach an acceptable level of operational readiness; to plan and direct military operations; and to assist in avoiding tactical, strategic, and technological surprises which may threaten U.S. vital interests at home and abroad.[3] At even higher levels of intelligence usage, many international negotiations, such as SALT and the Nuclear Test Ban Treaty, could not be undertaken without the support of sutiable intelligence.[4] While these examples do not list all of the myriad uses of intelligence that occur in the federal bureaucracy, they point to the fact that many of these activities could not proceed if the minimum amount of secrecy required for their success is not guaranteed. Admiral Stansfield Turner, the current Director of Central Intelligence, states that ". . . the American Intelligence Community has been the eyes and ears of the United States overseas for over 30 years" and concludes that if we cannot protect our intelligence sources and methods, our freedom, and perhaps our survival, may be in jeopardy.[5] In describing the dilemma of secrecy in our free society, former DCI William E. Colby quotes President Ford as saying, ". . . that he would be glad to share our secrets with 214,000,000 Americans if no further exposure would occur," yet there is no way to so inform the people of American without

informing the world at large.[6] One way or another, the ability of the United States to maintain even the barest minimum secrecy is now being questioned due to the so-called "hemorrhage of secrets" which assaults the eyes and ears of Americans -- and anyone else who may be interested -- on a daily basis.[7]

The Ship of State is Leaking

Although the phenomenon of "leaking" is probably as old as the profession of intelligence, the magnitude of this activity -- and what it portends for the Intelligence Community -- seems to have reached critical proportions today. Ambassador Frank Carlucci, the Deputy Director of the Central Intelligence Agency, says that he believes ". . . leaks now are the worst he has seen in 23 years of government service."[8] In discussing leaks which included the unauthorized disclosure of certain relations with Japan and South Korea, and new weapon systems as well as the identities of CIA operatives, Mr. Carlucci highlighted the diversity of the sources of leaks by saying that they stem from former CIA employees, current officials at the Pentagon and National Security Council, and from the Congress.[9] Although it be impossible to catalogue all of the reasons why various officials, in and out of government, decide to compromise national secrets, intelligence sources and methods, and all other manner of sensitive information, many leaks occur for political purposes and for the supposed gain which could accrue to the leaker on a

short-term basis.[10] At yet the other end of the leak spectrum, a whole category of unauthorized disclosures occurs in the belief that ideological purposes are served by exposing secret material and that any form of government secrecy violates the First Amendment guarantee of freedom of speech.[11] Amid the controversy over leaks, one former high ranking official of the CIA has even gone so far as to state that there "can be good leaks and bad leaks."[12] And surely we can all think of instances in the recent past which could be so characterized. The problem of leaks can then be seen as a multi-headed hydra inasmuch as each leaker probably believes that "his" leak is a "good" one and the other fellow's disclosure is a "bad" one that hurts the national security of the United States. At the federal level, the Congress blames the Executive for leaking policy sensitive information and, of course, the Executive blames Congress.

A member of the Senate Committee on Intelligence, for example, has recounted a situation in which he attended a top secret briefing concerning how certain U.S. intelligence collection activities would be impaired with the loss of various bases in Iran. The briefing included the steps being taken by the administration to supplement these losses with other collection methods. Inasmuch as the sites in Iran were used, in part, to verify Soviet compliance with SALT, the information was leaked the following day by administration officials in order to shore up dwindling public support for

the arms limitation treaty.[13] Perhaps this was the type of leak that David Wise was referring to when he quoted a high White House source as saying, "when we decide to make a leak, we make sure it does not jeopardize national security."[14] The perception, if not the fact, of a double standard concerning what is an "official" versus an "un-official" leak further exacerbates an already bad situation.[15] While some amount of leakage would seem to be inevitable in our society, the spate of leaks has even given rise to a blossoming cottage industry which trades on broken secrets.[16] As the institutional actors at the federal level continue to point accusatory fingers at one another in an effort to identify culprits, the overwhelming perception arises that the government has lost whatever ability it may have had to control official secrets -- and at least one result of this situation is the diminished ability of the U.S. Intelligence Community to protect its sources and methods.[17] The "great culprit hunt" has thus far identified few specific individuals guilty of leaking, yet it has identified at least three institutional mechanisms as possible accomplices: the 1974 Hughes-Ryan Amendment to the Foreign Assistance Act, the Freedom of Information Act, and the classification system.

The Hughes-Ryan Amendment

In 1974, Congress passed a little-noticed amendment to the Foreign Assistance Act which requires the President to report proposed sensitive intelligence operations to a number

of Congressional Committees. The amendment, of course, came about as a result of U.S. intelligence activities in Vietnam, Cambodia, Africa and elsewhere and reflected the sense of the Congress that the Executive should not undertake such acitivities, which could lead to wider U.S. involvement in the internal affairs of other nations, without the prior notification of Congress. This so-called Hughes-Ryan Amendment has now taken on proportions far beyond its original intent as it represents, at least in the minds of various Intelligence Community officials, the essence of the problem of guaranteeing the continued protection of intelligence sources and methods.[18] The Hughes-Ryan Amendment reads as follows:

Appendix I

Intelligence Activities and
Exchange of Materials

Sec. 32. The Foreign Assistance Act of 1961 is amended by adding at the end of Part III the following new sections:

Sec. 662. Limitation on intelligence Activities -

(a) No funds appropriated under the authority of this or any other Act may be expended by or on behalf of the Central Intelligence Agency for operations in foreign countries, other than activities intended solely for obtaining necessary intelligence, unless and until the President finds that such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of such operation to the appropriate committees of the Congress, including the Committee on Foreign Relations of the United States Senate and the Committee on Foreign Affairs of the United States House of Representatives.[19]

At the heart of the debate over the Hughes-Ryan Amendment is the belief that the President's responsibility for notifying the Senate Foreign Relations Committee and the House Foreign Affairs Committee, as well as other "appropriate" committees (which now include the House and Senate Armed Services, Appropriations and Intelligence Committees) of intended covert intelligence activities abroad, that the circle of individuals privy to the nation's most sensitive secrets can no longer be maintained.[20] This perception is based on the simplistic rationale that, ". . . as the circle of persons who know a secret widens, the likelihood of a leak increases until it becomes a virtual certainty."[21] And the Hughes-Ryan Amendment has theoretically widened the circle of persons with knowledge of covert activities to such an extent that the repeal of this amendment has become one of the Intelligence Community's first priorities.[22] Yet increasing the number of persons in the Congress who have access to such sensitive intelligence sources and methods data does not automatically mean that such information will, perforce, be disclosed in an unauthorized manner. It should be noted at this juncture that it is beyond the scope of this paper to examine the multiplicity of arguments that have arisen in conjunction with the Hughes-Ryan Amendment and that concern the highly charged and emotional considerations related to the pros and cons of engaging in covert intelligence operations at all.[23] Rather, the Hughes-Ryan Amendment has become

something of a strawman in the battle between the Executive/ Intelligence Community, on the one hand, and the Congress/ Oversight Committees, on the other hand, as to who is responsible for unauthorized disclosures -- and what can be done to reduce the number of leaks in order to protect intelligence sources and methods.

Contrary to the notion that a requirement to brief eight Congressional Committees and their staffs on sensitive intelligence data has increased the number of persons with such access to hundreds of people, the Hughes-Ryan requirement seems to have resulted in only a handful of Congressmen and a few staff personnel gaining such access.[24] And, according to one member of the House Intelligence Committee, no intelligence source and method data has leaked from those who have been briefed.[25] Yet a careful reading of the ill-fated attempts by the United States to aid the National Front for the Liberation of Angola in 1975 certainly suggests that the plan was quickly leaked to the press by a senator who was opposed to such activity.[26] Yet one known leak is certainly not a suitable sample upon which to conclude that a trend is in the making. It would then seem that the current battle to repeal the Hughes-Ryan amendment has at least certain characterisitcs of a facade being used for other political and intelligence purposes.

While it would appear that leaks and other unauthorized disclosures concerning intelligence sources and methods

probably emanate in equal numbers from both the Executive and Legislative branches, the Hughes-Ryan Amendment creates yet another category of risk impinging on the U.S. Intelligence Community today.[27] The amendment, for example, requires the President to personally certify to Congress that each covert action is "important to the national security of the United States." Without delving into the impact this action has on the oversight responsibilities which Congress has recently assumed, it should be noted that the United States is now probably the only country in the world which has stripped its chief executive of the ability to "plausibly deny" covert activity.[28] One need only recall the lost summit meeting after President Eisenhower took responsibility for the U-2 missions over the U.S.S.R. and the impact that President Kennedy's admission of responsibility for the Bay of Pigs fiasco had on both world affairs and U.S. intelligence activities to fully comprehend how the Hughes-Ryan Amendment threatens to reduce cooperative efforts with other friendly intelligence services.[29] Simply stated, the perception now exists that the United States cannot protect its intelligence sources and methods from public exposure and it is this perception, rather than the mechanics of the Hughes-Ryan Amendment itself, that has made the work of the U.S. Intelligence Community much more difficult. Admiral Turner, in describing the pervasive and pernicious nature of this perception, says that:

> Allied intelligence services are losing confidence that we can keep a secret (and that since I) must notify eight committees of Congress of every covert action . . . they could not imagine that the plan would not leak.[30]

The Freedom of Information Act

If the repeal of the Hughes-Ryan Amendment ranks first among the Intelligence Community's desires in order to improve its ability to protect sources and methods from unauthorized disclosure, gaining total exemption from the Freedom of Information Act (FOIA) is probably the number two priority.[31] The FOIA is thought to impinge on the Intelligence Community's problem of protecting sensitive sources and methods in a number of critical ways; and, as will be seen in the next chapter, it is closely related to the problem of using unclassified material in course of public trials of individuals accused of the unauthorized disclosure of such material. Perhaps more importantly, the FOIA, like the Hughes-Ryan Amendment, creates more of a perceptual problem for U.S. intelligence agencies than it does a problem of fact. This should not be construed to mean that perceptions -- and the domestic and international intelligence problems they create -- are somehow less important than other types of problems. Intelligence agencies depend on engendering the trust of those individuals who are both employed by them and those who cooperate with them.[32] Obviously, the perception of these sources concerning the Intelligence Community's interest and ability to protect them from unauthorized disclosure is just

as important as the objective facts which bound the problem. Once the perception exists that sources and methods could be exposed through FOIA actions, the Intelligence Community -- and the users and consumers of intelligence products -- suffers.

In contrast to the relatively narrow parameters of the Hughes-Ryan Amendment, the FOIA allows virtually anyone to request information from the government on just about any subject which may be in government files. It is important to note at this juncture that the U.S. Intelligence Community is the only intelligence system in the world requred by statute to produce information for outsiders on demand.[33]

In addition to private citizens and organizations within the United States who may request information for all imaginable purposes, the FOIA permits inquiries from foreigners as well, a fact that has not eluded the Polish and Soviet Embassies who have become regular requestors of information from U.S. Intelligence agencies.[34] Deputy CIA Director Carlucci sums up the problem by saying that "if the KGB were to write us (for information), we would be required to respond in ten days."[35] Yet in addition to Communist Bloc FOIA requesters, Brazil, Britain, Finland, Iran, Norway, Switzerland, West Germany, and France have been reported to be subscribing to cottage industry services within the U.S. which purport to provide all FOIA-related declassified documents for a fee of $16,000 per year.[36] The magnitude of the administrative burden which has arisen for U.S. intelligence agencies in

trying to catalogue the thousands of documents declassified under the FOIA becomes somewhat clearer with the knowledge that CIA, State, and Defense also subscribe to this same private service.[37] The importance of just keeping track of what information has come into the public domain is brought into sharper focus by the following notional analogy: a highly classified document, perhaps pertaining to U.S. military strategy, may be produced and disseminated in many copies. When such a document is declassified and made public through FOIA procedures, the holders of the remaining copies are not automatically notified of the declassification and continue to maintain their copies with the original classification. As time passes and literally thousands of other documents are declassified, it soon becomes impossible to determine that information remains validly classified and what does not. The staggering volume of material requested, approved, and disapproved each year under the FOIA precludes the implementation of any adequate notification system.[38]

In spite of the fact that private citizens and hostile foreign intelligence services may utilize the FOIA to gain access to previously denied information, the CIA does not claim that the FOIA has <u>directly</u> jeopardized its sources and methods of intelligence collection and analysis.[39] Indeed, the FOIA allows U.S. intelligence agencies and activities to deny requests for information if, <u>inter alia</u>, approval would threaten intelligence sources and methods, or validly classified

information, including information received from friendly foreign governments.[40] What does concern the U.S. Intelligence Community is that section of the FOIA which permits requesters, who have been denied information, to seek a rehersal on internal decisions to withhold information through litigation. Even though the FOIA has effectively substituted the public's "right to know" for the previous "need to know" principle,[41] the current DCI concludes that "we can't have 215 million Americans thinking they know what the United States national security interests are."[42] Moreover, the U.S. Intelligence Community fears that while individual bits of formerly classified data may pose little threat to current sources and methods, the vast and steady accumulation of information that has been made public since the FOIA came into being in 1966 tends to reveal a picture of the extent of U.S. intelligence activities and operations that severely cripples future operations.[43] This situation, added to the possibility of both incidental and accidental disclosures which have already occurred, strengthens the perception of intelligence officials here and abroad that secrets can no longer be protected under American law.[44]

The Classification System

Since its inception during the Truman Administration, the many rules, regulations -- and results -- of the government-wide classification system have been a subject of continuing controversy. Less than ten years ago it was estimated that

at least 38,000 persons in three government agencies had the power to wield a classification stamp. And it appears that they must have been a busy lot: 22 million documents were withheld from public scrutiny in the much-abused name of "national security."[45] The issues surrounding the classification system have probably been smoldering for years, but it was the publication of the Pentagon Papers in June of 1971 that unloosed the vigorous protest against wholesale government secrecy that resulted in the near-total revamping of the system that occurred in 1978.[46] Unfortunately, it would appear that although the procedures used to classify information have been changed, the end result is that millions upon millions of documents continue to be classified and hidden away in federal safes.[47] Without attempting to minimize the importance of the public's right to know what its government is doing, nor to maximize the necessity for some degree of secrecy in order to conduct government operations, the amount of material currently being classified can be described by no other term than ridiculous. Such flagrant abuses of secrecy breed not only arrognace and contempt on the part of government classifiers, it compounds the problem of protecting that small amount of information, to include intelligence sources and methods, which must validly be withheld from public view.[48] Simply put, ". . . when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those

intent on self-protection or self-promotion."[49] And that is exactly what has happened.

Classified information now enjoys little more real protection from unauthorized disclosure than any other form of data. Secrecy, says Stansfield Turner, has been used in the past to hide the Intelligence Community's mistakes and misdeeds, yet "in itself, secrecy is neither good nor bad, moral or immoral."[50] The real problem then, with secrecy and the classification system which allows such secrecy to proliferate, is that ordinary citizens become apathetic in terms of being able to differentiate between valid secrets and abuses of the system, leaks increase, and even noted journalists who have shown restraint in the past now feel unrestrained in regard to divulging classified information, even though national security might be at stake.[51]

While it is beyond the scope of this paper to analyse the classification system in full, it should be noted that the latest changes to this system attempt to correct many of the shortcomings associated with past classifications rules. Eleven agencies have had their previous classification authority withdrawn and at least five agencies have had their level of classification authority reduced. More importantly, the number of individuals with original Top Secret authority is now estimated at 1,400 out of over six million federal civilian and military employees (approximately 12,000 employees possess Secret and Confidential classification authority).

Some of the other changes in the "new" classification system include:

- o Requests for relase cannot be rejected merely due to the fact that a document is classified. A review must be made that the original reason for classification remains valid or the document must be released;
- o the General Classification System has been abolished and replaced with a system based on document content, a factor which will result in an additional 250 million pages being declassified over the next ten years (over and above the 350 million pages that would have been "normally" declassified);
- o the number of individuals authorized to declassify has been increased and an "Information Security Oversight Office" has been established to monitor declassification actions;
- o the use of classification to conceal violations of law is forbidden;
- o classification may not be restored to documents once they are officially relased to the public (this provision will be discussed in the next chapter as it relates directly to the problem of declassifying material for use in public trials of those accused of unauthorized disclosures); and
- o in order to be classified, documents must fall within one of seven categories of classification criteria and must represent an identifiable threat to the national security if disclosed.[52]

Yet the classification system retains the long familiar three-tiered categories of Top Secret, Secret, and Confidential which require the wholly subjective judgment on the part of classifiers that damage to the U.S. would be "exceptionally grave," "serious," or merely "identifiable" if the information were to be disclosed. Anyone familiar with past and present

classification rules is fully aware of the difficulty in trying to place information neatly into these categories, a situation that has frequently resulted in an abuse syndrome wherein individuals resolve the dilemma as follows: if in doubt, classify, and classify at the highest possible level rather than the lowest.[53] Although federal bureaucrats may be subject to any number of criticisms about their work habits, their ingenuity in devising ways and means to defeat the spirit and intent of the new classification system certainly cannot be ignored. In a recent report by the Comptroller General, the current classification system was being abused in the following ways:

- Information was classified by individuals who had no classification authority;
- individuals with top secret classification authority improperly delegated this authority to subordinates;
- internal agency classification guides did not specify limits on the use of derivative classifications;
- in one sample, 24% of the documents examined had been improperly classified in that they did not relate to national security;
- in another sample, 33% of the documents reviewed had deficient markings, i.e., failed to show the original classification authority or office, date for declassification or reason for classification was wrong, or the portions of the document that contained classified and unclassified information were not differentiated.[54]

Although the deficiencies cited by the Comptroller General are certainly serious in the aggregate, it may be that <u>any</u> attempt to systematically devise and implement a

classification program would suffer from the same defects. Individuals involved with classified information on a recurring basis tend to adhere to procedures which have been inculcated over time to the extent that they may, in fact, have become thoroughly internalized. Perhaps the types of administrative mismanagement so fully explored in the Comptroller General's report should be viewed through a framework which condones the fact that such errors may be inevitable. What should not be condoned is the fact that it now appears most leaks and other unauthorized disclosures of sensitive intelligence information stem from highly placed individuals in government who, on the one hand, bemoan the compromise of the sources and methods of this information while, on the other hand, they have become the very source of the compromise.[55] Even more critical to the future of the U.S. Intelligence Community's ability to protect its sources and methods is the building perception of a double standard when it comes to how high and low officials handle classified information.

A highly placed individual may, for example, selectively leak or disclose a piece of very sensitive classified information in order to float a trial balloon. Such an individual would not, of course, be prosecuted for such a disclosure, if he could be identified, in that he could validly claim that he was exercising his declassification authority. One can only rhetorically wonder about the fate of some lower level official caught in the same position.[56] When the minions

of the federal bureaucracy witness their elected and appointed leaders making such disclosures for political reasons it does not become difficult to understand why the classification system fails to achieve its intended purpose. A former CIA employee, for example, regularly participated in briefings wherein his superiors routinely leaked classified information to visiting Congressmen.[57] That same individual has now been convicted of violating the very same oath that he and his superiors signed in which they swore not to divulge information gained in the course of their employment. Other examples abound and they have not been missed by investigative reporters and other members of the press corps who are often accused of not respecting national security in that they publish every secret which becomes available. What is often forgotten is that the press created neither the information in question nor the system used to protect it in the first place.[58] The bottom line, says Frank Carlucci, is that there has been a severe "erosion of the environment for protecting national-security information . . . caused by leaks for policy reasons."[59]

CHAPTER VI

COPING WITH UNAUTHORIZED DISCLOSURES: PROBLEMS AND PROSPECTS

Investigating Unauthorized Disclosures

As the numbers, types and sources of unauthorized disclosures continue to increase, the pressures now being brought to bear on the various agencies with investigative responsibilities have increased as well. Former DCI William E. Colby reduces the problem of leaks and other forms of unauthorized disclosure to its basics when he says that "leakers should go to jail," and he is probably echoing a sentiment that many people in and out of the Intelligence Community would agree with.[1] Yet, as Mr. Colby is painfully aware, the difficulties associated with identifying the sources of unauthorized disclosures and successfully bringing them to trial have themselves become an integral part of the problem of protecting intelligence sources and methods. The frustration on the part of the government in dealing with unauthorized disclosures comes through clearly in the statement of two officials who have been investigating this phenomenon when they say that the government continues to look for that quintessential case in order to ". . . make an example -- a case that would really slam an employee. . . ."[2]

Limitations on the Authority of the Director of Central Intelligence. In order to coordinate the intelligence functions of the federal government, to include the correlation,

evaluation, and dissemination of intelligence affecting U.S. national security, the National Security Act of 1947 created the Central Intelligence Agency and charged the DCI with the responsibility for the protection of intelligence sources and methods. Although Title 50 USC Section 403(d) simply states "that the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure," a reflection of Congressional awareness that intelligence functions necessarily involve sensitive materials and that secrecy is critical, it does not provide the DCI with any guidance on the scope of this responsibility nor how it should be discharged.[3] Indeed, the statute, and the legislative debates associated with its passage, conspicuously limit the DCI's authority to protect sensitive intelligence sources and methods. The act specifically provides that the CIA and the DCI shall have no law enforcement powers nor domestic security functions and reflects a sense of Congress that CIA activities in the United States would only be permitted to the extent that they supported the CIA's primary foreign intelligence mission.[4] In 1972, the National Security Council attempted to clarify the DCI's responsibilities for the protection of intelligence sources and methods by issuing an intelligence directive which states, in part, that:

> The director of Central Intelligence, with the advice of the United States Intelligence Board, shall ensure the development of policies and procedures for the protection of intelligence and

> intelligence sources and methods from unauthorized disclosure. Each department and agency shall remain responsible for the protection of intelligence and intelligence sources and methods within its own organization. Each shall also establish appropriate internal policies and procedures to prevent the unauthorized disclosure from within that agency of intelligence information or activity. The Director of Central Intelligence shall call upon the departments and agencies (of the Intelligence Community), as appropriate, to investigate within their department or agency any unauthorized disclosure of intelligence or of intelligence sources and methods. A report of these investigations, including corrective measures taken or recommended within the departments and agencies involved, shall be transmitted to the Director of Central Intelligence for review and such further action as may be appropriate, including reports to the National Security Council or the president.[5]

Although there would seem to be little purpose in reopening the wounds associated with the sensational disclosure of the many abuses of power and authority attributed to the Intelligence Community in recent years, it should be noted that at least some of these abuses stemmed from wholly misguided perceptions by officials in the Intelligence Community, and elsewhere in government, of what constituted valid legal measures to protect intelligence and sources from unauthorized disclosure. While much has changed in the past few years, the legacy of suspicion surrounding past illegal telephone taps, burglaries, and unsubtantiated intrusions of privacy continues to impede the adequate protection of intelligence sources and methods today. In regard to investigating the unauthorized disclosure of classified material, a careful and critical line has been drawn between the responsibilities of the DCI and the Federal Bureau of Investigation (FBI).[6]

Investigative Anomalies. Leak investigations typically begin when an employee within the Intelligence Community identifies a possible leak on a subject with which he is familiar. This normally occurs when the information in question is published om or is otherwise exposed through another medium. The individual then notifies his office of security of the alleged leak and an attempt is made to determine the individuals or offices who had access to the information in question. Not unexpectedly, this initial investigative effort often proves useless due to the relatively wide dissemination of interagency classified materials. CIA intelligence cables, the National Intelligence Daily, and the Weapons Intelligence Summary, for example, may have government-wide distribution lists which include thousands of readers -- all authorized to receive them and all potential leakers. And it is the very sensitive material which must be used by policymakers -- and thus requires the greatest amount of protection -- that is often the most frequently compromised.[7]

As the internal investigation continues, the agency responsible for the original production of the intelligence is tasked with preparing a damage assessment. The difficulties of trying to assess the damage to the United States and its intelligence sources and methods from unauthorized disclosures are manifold: it is often impossible to determine if a foreign power has become aware of the exposed material and, if they are, what steps might be taken by them.[8]

During World War II, for example, the Chicago Tribune published a story concerning the fact that the U.S. armed forces had somehow broken the Japanese code because we knew the location of their ships. Had current damage assessment procedures been used at that time, a unanimous decision would probably have been reached by all concerned that inasmuch as the Japanese would now change their codes and associated cryptologic systems, that the war effort of the U.S. had been gravely impaired. After the war it was learned that the Japanese did not read the Chicago Tribune and, of course, did not change their codes.[9] The same sort of anomaly occurs today when a former CIA employee publishes the names of current CIA operatives based on information already in the public domain or the Intelligence Community loses a technical manual for a surveillance satellite and admits that the loss has gone undetected for years.[10] Although these extreme examples probably have had a real and critical impact on the Intelligence Community's ability to protect sources and methods, and may have resulted in the death of at least one CIA employee, they highlight the problem of trying to assess the potential damage of unauthorized disclosures.[11] The appearance, if not the fact, of the Intelligence Community continuing to abuse its authorities in the name of national security, even when a direct link between its sources and methods and the security of the nation is clear, has lead to both perfunctory damage assessments and the disillusionment of journalists who now publish classified data with impunity.[12]

When the damage assessment is completed, it is normally forwarded to the agency or department responsible for producing the leaked document and to the DCI's Security Committee, an interagency body composed of a small standing staff who regularly meet with security officials throughout the Intelligence Community. Oftentimes leak investigations end at this point when a determination is made that, due to wide dissemination, further investigative activity would be fruitless. If, however, a decision is made to continue the investigation, the damage assessment is then forwarded to the Justice Department with an accompanying request for further investigation.[13]

The Security Committee's request is just that: it has no authority to direct an investigation by the FBI or any other agency for that matter. In the past, the FBI would not accept "leak" investigations unless directed to do so by the Attorney General. This was a reflection of then FBI Director Hoover's belief that such investigations were ". . . an inappropriate use of FBI resources, because most of the time the source of the 'leak' could not be discovered, and often when the source was discovered, it turned out to be a high-ranking official against whom no action would be taken."[14] Under presidential pressures, the CIA and the Intelligence Community then often undertook these investigations themselves, relying on the "sources and methods" proviso of the National Security Act for authority. While

much has changed since the death of J. Edgar Hoover and the disclosure of intelligence abuses, the problem of investigating leaks still persists.

When the FBI now receives a request from the Intelligence Community to investigate an alleged leak, it does not automatically turn the request down. Rather, the FBI responds with what has become known as the infamous "11 Questions." Some of the 11 Questions are uncontroversial in that they deal with such subjects as whether the disclosed data was classified, accurate, and what document it may have come from, to include the name of the individual responsible for its security. Other questions concern the extent of dissemination and whether the document had been the subject of prior release requests, perhaps under the FOIA or through normal declassification procedures. One question deals directly with the effect that the disclosure of the classified data could have on the national defense -- and this is one reason for the preparation of damage assessments discussed earlier. Yet it is the ninth question which creates serious dilemmas for the Intelligence Community in that the response to it is often the key to whether a leak investigation will proceed. The ninth question asks "whether the data can be declassified for the purpose of prosecution and, if so, the name of the person competent to testify concerning the classification."[15] The Intelligence Community has come to view this question as a requirement that they must agree to

declassify exposed material first or the FBI will decline the case; it also presents something of a Catch-22 situation: to what extent must the national security be further harmed in order to protect the national security?[16]

In cases where espionage is involved or susptected, that is, classified information has been covertly passed to agents of a foreign power, investigative activity is undertaken much more seriously and vigorously. Interestingly, the FBI does not use the 11 Questions in such cases even though espionage and leak cases can be prosecuted under the same criminal statutes. In such cases the Justice Department and Intelligence Community officials often work out ad hoc arrangements in order to avoid the initial impasse in leak cases concerning the willingness to declassify information before proceeding with an investigation and trial.[17] The reasons for this working accomodation can only be surmised. It may be the view of the officials concerned that, while leaks outnumber instances of espionage by orders of magnitude, espionage may be considered an intrinsically more serious offense. Such a view may logically appeal to many people who, of course, abhor the idea of foreign or domestic spies in our midst, yet the cumulative effect of the continual flow of classified information to the public and world at large can reasonably be considered an equal threat to both U.S. national security and intelligence sources and methods. Another reason which may impact on the decision of the Justice

Department to avoid leak investigations in favor of espionage cases is that the current administration has gone on record in support of "whistle-blowers" and to pursue leakers with zeal could create the image of the government harrassing the very people it wishes to support. The bottom line, however, would still seem to be the fact that, because of the hugh number of leaks; investigating all of them would mean, in the words of one Justice Department official, that ". . . we would have little time to do anything else if all of them were followed up."[18] In any event, few, if any, leak cases have ever resulted in prosecution and certain espionage cases have been voluntarily dropped by the government. Indeed, in one instance an espionage case was dropped and no punitive action was taken even when the suspect readily admitted to the charge.[19] As oftentimes happens, cases that are dropped frequently involve high-level government officials guilty of leaks, or espionage cases involving lower-level federal employees. According to a former chief investigator for the Department of Defense, there are only two conditions under which a leaker can get into trouble: "When the leaker is a person of no importance and when the leaker has no important friends."[20] This same investigator goes on to cite the case of an individual who, prior to assuming a position as a Deputy Secretary of Defense, had been the subject of 22 separate investigations involving the leak of top secret material involving U.S. SALT plans and

strategies. In that case, higher level officials intervened to curtail prosecutorial action.[21] In addition to such political reasons as the cause for this selectively lackluster interest in actively pursuing unauthorized disclosures, another common denominator is the fear of Intelligence Community officials that, due to the wide-ranging nature of a suspect's access to other classified information, prosecution could result in the exposure of far more classified information. This phenomenon has given rise to the neologistic term "graymail" and is closely associated with the overall dilemma of to "disclose or dismiss."[22]

Graymail and Other Prosecutorial Dilemmas

Graymail. One might think that if the rocky road of bureaucratic obstacles and hurdles that is traversed in the early stages of an investigation concerning leaks or espionage could be surrmounted, and indeed merely identifying the culprit is no small task, that taking the suspect to trial would be the easiest part of the procedure. But it is at this point in the overall process of protecting intelligence sources and methods that many of the most difficult decisions must be made and Faustian bargains concluded. A former General Counsel for the CIA aptly notes that:

> When you embark on one these (leak or espionage) prosecutions, you are buying a ticket to go down a very long and difficult road, and at that moment you really can only see the first few feet of the way. You do not know what lies beyond. You do not know how the case is going

> to be defended. You do not know what discovery will be directed against you or how far it will be allowed by the judge, or under what rulings the judge is going to make or even what issue he will have to rule on. Much of that is unknowable and unforeseeable when these cases begin.
>
> You can say that the Government always has the ultimate trump in these situations because if the disclosure demands mount up too high and if the going gets too tough, you can always back out. The prosecution can always be dismissed. But I want to assure you it is not that simple because these cases, once they are started, tend to develop a great deal of momentum. Some are very, very important cases in which the interest in success is very high and compelling, and it always seems when you have started on this course that it is better, more prudent, to give up the one additional piece of information that is being asked, hoping that that will end it rather than quit the whole process. Plus, if you ever play that trump and back out of one of these things, you have to understand that at that point there will develop a very considerable pressure to understand why it happened. The press will want to know if the case goes down for national security reasons, what the reason was, and they will scan around looking for the particular reason, and indeed, by backing away, you can very well achieve what you are trying to avoid, which is more highlighting on your problem and enhanced likelihood that the information will come out through another channel.[23]

While the government may hold the ultimate trump card in these cases in that they can seek a dismissal if "the going gets too tough," defendants are not entirely without recourses and trump cards as well. Defendants can also, of course, seek dismissal on the basis of the weakness of preliminary evidence put forth by the government, yet such successes have been few. A much more potent trump card in the arsenal of defense of those accused of unauthorized disclosure is to

rely on the pertinent sections of the Federal Rules of Ciminal Procedure pertaining to discovery and inspection. These procedures generally allow defendants to request (a) all materials obtained from or belonging to the defendant; (b) anything "material to the preparation of his defense;" (c) information pertaining to the testimony of a government witness; and (d) any exculpatory information within the government's possession. As often happens, much of this information is classified and would be disclosed either during the trail or during pre-trail hearings.[24] A defendant's intention, or merely his threat, to use discovery procedures in order to obtain and expose additional classified material should his trial continue has come to be described as "graymail."[25]

Eventhough the term "graymail" may sound like a new addition to a vocabulary accustomed to catchy phrases and all-encompassing labels, the phenomenon is certainly not new. In 1807, for example, Aaron Burr's attempt to subpoena the President was upheld in the Supreme Court on the basis of Burr's Constitutional right to <u>any</u> information in the possession of the government which he may have needed to mount a successful defense against the accusation of having breached national security.[26] In more recent times, individuals accused of similar crimes have often used these same Constitutional guarantees to intimidate the government into either dropping the case or granting immunity from further prosecution.

What is new, then, is the increasing number of cases of graymail which now occur -- and how successful the tactic has become.

"Disclose or Dismiss." Although graymail has come to take on perjorative connotations when it appears that Constitutional guarantees often result in the dismissal of leak and espionage cases, it must be pointed out that graymail cannot be viewed solely as an unscrupulous or even questionable defense tactic. In many cases, a defendant is simply exercising his legal right to seek and obtain pertinent information, even though it may be classified, that is highly relevant to his defense. Whatever the motivation, defendants who use these procedures, and implicitly or explicitly threaten to expose more classified material, create serious dilemmas for the government which has the responsibility to insure that the law is equally and fairly enforced, on the one hand, and to insure that the nation's security is protected, on the other hand.[27] This balancing act creates the "disclose or dismiss" dilemma described as follows by an Assistant Attorney General:

> To fully understand the problem, it is necessary to examine the decision making process in criminal cases involving classified information. Under present procedures, decisions regarding the relevance and admissibility of evidence are normally made as they arise during the course of the trial. In advance of the trail, the government often must guess whether the defendant will seek to disclose certain classified information and speculate whether it will be found admissible if objected to at trial. In addition, there is a question

> whether material will be disclosed at trail and the damage inflicted before a ruling on the use of the information can be obtained. The situation is further complicated in cases where the government expects to disclose some classified items in presenting its case. Without a procedure for pre-trial rulings on the disclosure of classified information, the deck is stacked against proceeding with these cases because all of the sensitive items that might be disclosed at trail must be weighed in assessing whether the prosecution is sufficiently important to incur the national security risks.
>
> In the past, the government has foregone prosecution of conduct it believed to violate criminal laws in order to avoid compromising national security information. The costs of such decisions go beyond the failure to redress particular instances of illegal conduct. Such determinations foster the perception that government officials and private persons with access to military or technological secrets have a broad de facto immunity from prosecution for a variety of crimes. This perception not only undermines the public's confidence in the fair administration of criminal justice but it also promotes concern that there is no effective check against improper conduct by members of our intelligence agencies.[28]

And it would seem that the "disclose or dismiss" dilemma is often resolved in favor of the latter in many cases. A recent report of the Senate Select Committee on Intelligence, which made an exhaustive study of the relationship between national security secrets and the administration of justice, concluded that "there has been a major failure on the part of the Government to take action in leak cases."[29] The report went on to list a number of specific cases in which the use of graymail had been employed to persuade, cajole, or otherwise pressure the government into dropping prosecutions.[30] This same report parenthetically notes that certain leak and

espionage cases, which were dropped, were not included as they would raise the same security considerations as did the investigations or prosecutions -- further exposure of legitimate national secrets.[31] Graymail and the disclose or dismiss dilemma are generally considered to fall under the overall rubric of those factors which tend to augment the potential damage to intelligence sources and methods as a part of judicial proceedings. Another category closely associated with judicial augmentation threats to national security occurs through the possibility of "confirmation."

Damage by Confirmation. The successful investigation or attempted prosecution of leakers and spies can further weaken the Intelligence Community's ability to protect sources and methods by inadvertently confirming the validity and accuracy of the exposed information. In the case of the clandestine passing of defense secrets to a foreign government or the leak of the very same information, for example, recipients may tend to discount the data because of questions about the reliability of the source, whether it be a spy or a newspaper. Yet if an indictment is filed against this same source of the unauthorized disclosure, foreign intelligence services may then be persuaded that the information in question is, in fact, accurate. This type of confirmation damage to intelligence sources and methods may be impossible to remedy due to the Sixth Amendment guarantee of an open trial. Conformation problems also occur when, in the course

of an investigation or trial, additional classified information is exposed to either the defendant or potential witnesses to further the investigation or to prove the case. It is often necessary in the course of an investigation to discuss the known facts of the case with a number of witnesses who may or may not agree to protect the very type of information that is threatened. This threat is particularly troublesome in espionage cases where a prosecutor may disclose sophisticated -- and current -- counterespionage methods.[32] It would also seem that the problem of confirmation works both ways: the validity of exposed information may be confirmed if a prosecution is pursued and if it is dropped. The latter paradox would occur when a highly publicized case involving sensitive intelligence materials is dismissed through a government-initiated request based on national security considerations.

Other Judicial Procedural Considerations. In order to cope with the seemingly endless list of judicial obstacles in the path of the government when attempting to prosecute unauthorized disclosure cases, a number of innovative, albeit ad hoc, techniques have been devised by the Intelligence [illegible]mmunity and the Justice Department. Some of these pro[illegible]es have been more successful than others in that, inas[illegible] a formal basis in law, they depend on each [illegible] philosophical frame of reference for [illegible]ngs. This situation, of course,

often results in reluctance on the part of the Intellience Community to press for a trial and conviction in the most egregious cases of compromised classified material. Such cases create the dilemma of the need to punish gross offenders while concurrently threatening the exposure of the most sensitive source and method information at the same time. Chief among the ad hoc procedures often attempted by the Intelligence Community and Justice Department officials in these instances are ex parte and in camera hearings with the trial judge.[33]

Considering the fact that the legal community continues to debate the legality and propriety of many of the judicial procedures which have been attempted in the recent past when cases involving national security information come to trial, no attempt is made herein to provide "the final word" about these procedures. Rather, the purpose is only to familiarize the reader with the fact that while many Intelligence Community officials may paint an overly pessimistic picture of the perils and pitfalls they confront in prosecuting sensitive cases under the American concept of jurisprudence, these same officials have also enjoyed some rather important, perhaps even extraordinary, successes as well.

In essence, ex parte (Latin from or on one side only) and in camera (also from the Latin, meaning in private or in chambers) procedures involve moves on the part of Intelligence Community and Justice Department officials to seek

pre-trial meetings with presiding judges in order to avoid, or minimize, the dilemmas created by the threat of graymail and not be confronted with a disclose or dismiss situation as a trial proceeds. In ex parte procedures, the defendant and his counsel are excluded from private, or in camera meetings with trial judges and involve government attempts to obtain early rulings on such crucial matters as the relevancy of defense requests for classified or sensitive materials under the federal rules for discovery discussed earlier. It is also the aim of federal prosecutors to attempt to learn at this time how a judge may construe the question of classification validity. Obviously, if the government wishes to prove that the national security has been somehow harmed by the disclosure of classified information, the fact of its classification, as well as the validity of that classification, will impact the case in a number of ways. Moreover, ex parte and in camera procedures often involve attempts by prosecutors to establish other ad hoc procedures, such as the willingness of a judge to accept the redaction of classified documents as evidence in order to allow the prosecutors to avoid the pitfall of having to introduce a full document into evidence at trial when only a few pages of that document are pertinent. Prosecutors may also seek protective orders governing the procedures to be used in handling classified information at trial. These orders include such things as who can gain access to the material,

the circumstances of such access, how classified material will be stored, and the disposition of classified material at the conclusion of the trial. In espionage cases, wherein the FBI's 11 Questions have not been used before a trial begins to ascertain the willingness of the Intelligence Community to declassify information so that it may be introduced as evidence, federal prosecutors have often succeeded in obtaining judicial approval to declassify certain data, place it under restrictive protective orders to limit its exposure, and then turn it back over to the Intelligence Community for reclassification at the end of the trial. How this procedure is reconciled with the earlier noted provision of the Executive Order on the classification system, which prohits the reclassification of information once made public, continues to be a matter of heated debate.[34]

The problems and prospects which the above procedures engender are without limits. As has happened in some cases, trial judges have accepted and implemented some, or all, of these procedures in order to conduct as fair a trial as is humanly possible while concurrently recognizing the need to protect classified information and intelligence sources and methods from needless further exposure. Other judges have steadfastly refused to recognize classified documents, which the government or defendants must use at trial, as requiring any different procedures than would be required under the rules of evidence.[35] Judges in the latter category apparently

subscribe to the belief that defendants accused of having breached the national security are precisely those most in need of the fullest legal guarantees afforded by the laws in being. In speaking of the dilemma wrought by the need to divulge state secrets which may imperil national security, a former Supreme Court Justice makes a cogent argument against many of the aforementioned evidentiary and procedural privileges used by the Intelligence Community and the Justice Department in the past:

> Few weapons in the arsenal of freedom are more useful than the power to compel a government to disclose the evidence on which it seeks to forfeit the liberty of its citizens. All governments, democracies as well as autocracies, believe that those they seek to punish are guilty; the impediments of constitutional barriers are galling to all governments when they prevent the consummation of that just purpose. But those barriers were devised and are precious because they prevent that purpose and its pursuit from passing unchallenged by the accused, and unpurged by the alembric of public scrutiny and public criticism. A society which has come to wince at such exposure of the methods by which it seeks to impose its will upon its members, has already lost the feel of freedom and is on the path towards absolutism.[36]

While precedent for or against evidentiary and procedural manipulation has been accumulating in the past few years, the overall problem continues to be of national security roulette when classified information and intelligence sources and methods may be exposed in the course of a trial. All of the aforementioned prosecutorial dilemmas notwithstanding, one of the most critical issues confronting the Intelligence Community is the status of that body of law upon which many trials

involving unauthorized disclosure are based: the highly controversial Espionage Laws.

The Special Case of the Espionage Laws

It is a likely probability that most people in government who, at one time or another, have been approved for access to classified information have signed some form of oath or secrecy agreement. The completion of these agreements, inter alia, often signifies that the individual will protect classified information and that he has read and that he understands his obligations under the espionage laws concerning the unauthorized disclosure of defense and defense-related materials. These laws came into being at about the time of the United States' entrance into World War I and, with few exceptions, have remained unchanged in a constantly changing world. More than 60 years have passed since the enacement of the Espionage Laws, and the dialogue concerning the precise meaning of these laws, as well as their application, continues unabated and unresolved. Congress has totally avoided clarifying the ambiguities in the espionage laws primarily because of the impossibility of trying to distinguish between a criminal act -- espionage -- and what has widely become an accepted governmental practice -- leaking of classified information. While leaks and espionage are, of course, qualitatively different, the end result is often the same: the national defense of the United States is weakened by the universal exposure of state secrets and the sources and methods

used to accumulate and analyze them. Yet many attempts to amend or replace the espionage laws have floundered at least in part because Congress has been reluctant to explicitly make leaks of classified information a criminal act.[37]

One of the truly interesting paradoxes in American life appears to be the overwhelming support that the majority of citizens evidence for the abstract idea of freedom of speech and thought while concommitantly denying this principle in practice. Without attempting to second guess the framers of the Constitution, it seems clear that the First Amendment was specifically intended to prevent the government from curtailing free expression, however alarming or distasteful such expressions may be -- and regardless of the risks to national security that might accompany such expression. Yet, says Peter S. Prescott in his recent review of Nat Hentoff's new book The First Freedom: The Tumultuous History of Free Speech in America, "Bill of Rights or no, the American tradition is to revere freedom of speech except for those with whom we disagree."[38] And since Americans in general, and the Intelligence Community specifically, reject leaks and other forms of unauthorized disclosure, including whistle-blowing and the exposure of government exesses kept secret by the classification system, as valid forms of public expression, many attempts to make the espionage laws a more useable tool have been predicated on British Official Secrets Act.[39]

Like Clausewitz' On War, and perhaps even our own espionage laws, the British Official Secrets Act is one of the most quoted and least read and understood of documents. This may be due to at least the appearance in the British model of the government having the means to control its secrets, to protect its intelligence sources and methods, and to avoid the perception now impinging on U.S. Intelligence activities that everything will eventually leak -- either through litigation or unauthorized disclosure. And there is much in that perception which is true. Yet the Official Secrets Act not only applies to a nation with a quite dissimilar constitution, no Freedom of Information Act and no Hughes-Ryan Amendment, it also applies to divulgence or publication of all government information, not just national security secrets.[40] In addition to the selective application of the Official Secrets Act in Britain, as well as the question of the constitutionality of such a law in the U.S., an official secrets act will not resolve or ameliorate the problems associated with graymail.[41] For these, and many other reasons, the likelihood of enactment of a similar law in the United States seems slight -- as well it should be.

Recognizing that the Espionage Laws of the U.S. can probably not be replaced in toto, two eminent professors of law at Columbia University have completed an exhaustive study of these and related laws in order to underscore their difficiencies in both scope and content. These jurisprudential

scholars, whose study ran to more than 150 pages and has become something of a classic for those interested in the subject, concluded that:

> The basic espionage statutes are totally inadequate. Even in their treatment of outright spying they are poorly conceived and clumsily drafted.[42]

These two scholars went on to catalogue myriad other anomalies and enigmas extant in the Espionage Laws, most of which center on the imprecise meaning of the laws and the fact that they often require the government to prove intent to willfully injure the United States. They further contrast these provisions of the law with other sections which compound the problem of determining whether the publication of leaked secrets constitutes "intent to injure" or merely the exercise of First Amendment rights.[43] The bottom line, however, is that this study has put to rest the legal neophyte's hope, if not belief, that the publication -- in any form -- of defense secrets is a punishable offense. As long as direct contact with an agent or agents of a foreign power cannot be conclusively proven, unauthorized disclosers of classified material and intelligence sources and methods have little to fear from the Espionage statutes.[44] For this reason, when no such link can be conclusively proven, the Intelligence Community often must attempt prosecution under other sections of the criminal or civil code, or, as has become much more frequent, rely on a variety of administrative sanctions to stem the tide of unauthorized disclosures.

Secrecy Oaths and Administrative Remedies

The increasing number of unauthorized disclosures, as well as the possibility of "authorized" disclosures associated with attempts to bring suspected violators to trial has led Intelligence Community and Justice Department officials to often eschew criminal proceedings in favor of civil suits or the use of administrative sanctions. Although the Director of Central Intelligence certainly has limited authority in discharging his statutory responsibility to protect intelligence sources and methods from unauthorized disclosure, he has, in the words of Senate Select Committee on Intelligence, ". . . extraordinary powers under the 1947 National Security Act . . ." and it appears that these powers are being exercised in more and more instances.[45]

Perhaps one of the most important authorities possessed by the DCI is his authority to summarily discharge current employees without recourse to often long and tedious civil service procedures. The DCI has exercised this option in recent years, however, in the case of one employee who was fired from the CIA after confessing that he provided copies of top secret CIA reports to a senatorial staff aide, no federal law was violated and the individual was subsequently hired by yet another senator. Although the CIA eventually recovered the classified documents, they did contain extremely sensitive information about intelligence sources and methods that can be expected to make their way into the public domain if the

now-defunct debate over the SALT II agreements reemerges in Congress. Finally, it should be noted that the individual who leaked these documents has had his security clearances reinstituted.[46]

In the case of former employees of the CIA, secrecy oaths signed as a condition of employment have proven far more successful in terms of punitive actions taken by the Intelligence Community to stem the tide of leaks. These oaths, which have undergone a number of permutations and combinations over the years in order to keep up with the leak phenomenon, generally stipulate that individuals employed by the CIA must agree not to divulge any information about intelligence or intelligence-related activities which they may have learned during the course of their employment. Furthermore, CIA secrecy oaths require that individuals who intend to write articles about intelligence must submit their manuscripts to the CIA for review and a determination that they do not contain classified information.[47]

Over the past ten years, there have been a number of precedent-setting cases concerning former CIA employees who have failed to abide by their secrecy agreements -- at least in the opinion of the DCI and the courts which have decided many of these cases. In prosecuting these cases, the Intelligence Community has steadfastly relied on civil law rather than open the Pandora's box of trying to prove intent to injure the United States as required under the espionage

statutes. These cases, which depend on simple breach of contract requirements in civil law as the basis for culpability, have also raised an interesting number of other issues concerning America's ability to protect intelligence sources and methods from unauthorized disclosure.[48]

In addition to the obvious problem of whether or not an individual can, in fact, waive his First Amendment rights at all, the use of breach of contract suits in violation of secrecy oath cases are only applicable to those relatively small number of Intelligence Community current and former employees who have signed them. Although there was an attempt to require all persons granted access to classified material to sign oaths similar to the CIA's secrecy agreement when the Executive Order on the classification system was redrawn, it was dropped from the final version due to the Constitutional uproar such a requirement would engender.[49] In essence, then, this avenue to protect intelligence sources and methods is, by definition, extremely narrow in its application and runs the risk of criticism due to its highly selective application. Although the DCI has been able to unequivocably prove his right to the prior review of articles written by former CIA employees, it is difficult to imagine how these reviews can do more for the protection of intelligence sources and methods than keeping the honest people honest. This is due to the fact that most cases that come to trial have involved materials that have already been published and are in the public domain.

Court decisions in favor of the government and the Intelligence Community often involve no more than pecuniary damages and court orders which reaffirm the original stipulations of the secrecy agreement if the author should attempt to publish again. Yet the original information upon which the case was based has been made public and can no longer be reclaimed.[50]

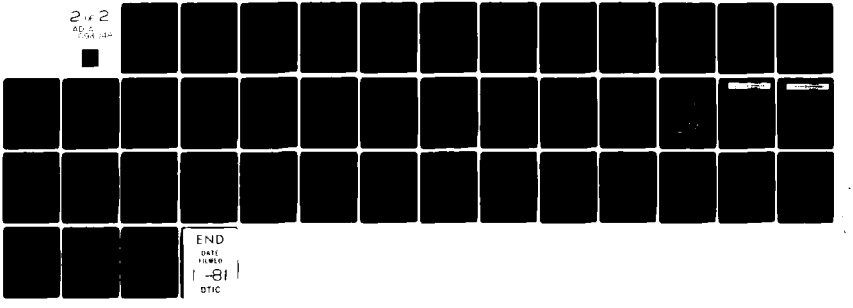
CHAPTER VII

CONCLUSION

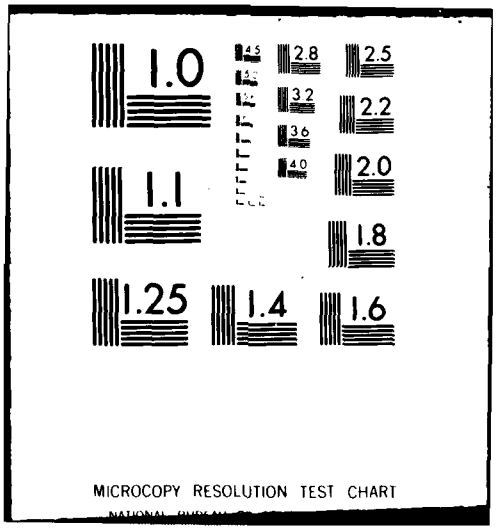
In writing about the Intelligence Community, the first problem which must be confronted is the one that all authors probably face: what to include or exclude. Human nature being what it is, this study focuses attention on just a few of the myriad problems which affect the production of intelligence today. The choice of subjects which have been included herein are wholly subjective; the list could have been much longer or shorter. The problems chosen for examination are the ones that have been of the most concern to the author as a professional intelligence officer for more than 16 years; their significance will, of course, vary with the perceptions which the reader will bring to this study. Since "intelligence" touches all of our lives in both personal and professional ways, few readers will be without opinions concerning how well intelligence does its job. This ubiquitousness of intelligence also produces yet another phenomenon: everyone has ideas about how to "improve" intelligence organization, products, or management. No such claim to expertise is found in this study. Because the underlying premise of this study is that intelligence structures and functions have been, and will continue to be, integral parts of each nation's struggle for survival, the purpose of the study has been to highlight and illuminate some of the more visible factors which now threaten the U.S.

AD-A093 048 NAVAL WAR COLL NEWPORT RI CENTER FOR ADVANCED RESEARCH F/G 15/4
THE U.S. INTELLIGENCE COMMUNITY: DILEMMAS OF MANAGEMENT AND LAW--ETC(U)
JUN 80 W H MILBERG

UNCLASSIFIED NL



END
DATE FILMED
-81
DTIC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
MICROCOPY RESOLUTION TEST CHART

Intelligence Community's ability to provide a unique service to the nation. Rather than try to provide a rigorous or comprehensive list of solutions, it is hoped that some of the ideas put forth will inform those who may have come to take intelligence for granted of the many organizational and legal issues pertinent to intelligence production.

The Intelligence Community, in its current configuration, is just a little over two years old and bears little resemblance to any other governmental entity. Since the surprise attack on Pearl Harbor nearly forty years ago, various attempts have been made to organize and implement a truly central intelligence system in the United States. That objective continues to be elusive. On the one hand, a Director of Central Intelligence must be the executive head of the CIA, the government's senior intelligence official, and the leader of the Intelligence Community. These roles are often mutually exclusive and present serious problems in terms of the inherent struggles for power and budgetary control which have ensued. The limited authorities and responsibilities of the DCI, for example, in attempting to orchestrate the budget, priorities, and intelligence production responsibilities for the Intelligence Community basically necessitate the use of less than perfect means to accomplish these aims. This is due to the fact that many of the DCI's responsibilities are, in fact, shared with a number of other senior officials who either are cabinet members or control large

portions of national intelligence assets -- or both. On the other hand, our pluralistic society may not, in the face of the sensational revelations concerning the abuses of intelligence power which occurred just a few short years ago, support the centralization of any more power in the hands of a single invididual. It may be that the present structure of the Intelligence Community, to include the various committees, centers, and boards each having a specific piece of the intelligence action, is the best organizational structure that can be designed considering the needs of both users of intelligence and long-standing public wariness about secret organizations in an open society.

With the notable exception of the CIA, none of the agencies, departments, or elements which comprise the Intelligence Community have a legal charter for their organizaion or operation. The CIA's charter was enacted in the post-WWII era and at a time when the cold war was already in full swing. Much has changed in the interim. Attempts to enact comprehensive charters for all components of the Intelligence Community, that recognize and consider the need for a legally based U.S. intelligence system, continue to founder on the shoals of day-to-day politics and near-term world events. Charter legislation is, of course, a dual-edged sword: while it would for once minimize the overlap and duplication which now characterize many Intelligence Community activities, it would also reduce flexibility since roles and missions would

be locked in law and not subject to change by executive fiat. While the Intelligence Community has generally been opposed to legal charters due to fears of too restrictive legislation, it has been an ardent supporter of many of the concurrent attempts to legislate protective measures for its sources and methods.

The internal battles over intelligence management and organization are matched in their vociferousness and import by the external battles concerning the Intelligence Community's ability to protect its sources and methods. Leaking -- for whatever reason -- has become a political institution in the United States and shows no sign of abatement. The unauthorized disclosure of sensitive intelligence materials is abetted by unforeseen accomplices, such as the Hughes-Ryan Amendment, the Freedom of Information Act, and perhaps most importantly, a government-wide classficiation system which engenders little respect. Investigating and prosecuting those guilty of jeopardizing this nation's most important intelligence secrets has created yet other categories of dilemmas in the courtroom and elsewhere. World War I vintage Espionage Laws may have offered some modicum of protection for the nation's secrets in 1917, but in 1980 they are little more than a confused amalgamation of legal mumbo-jumbo and, as such, are rarely used in cases involving the unauthorized disclosure of intelligence sources and methods. In their stead, a full panoply of administrative remedies has been devised to fill

the legal void, each creating its own record of successes, failures, and additional dilemmas in its wake. Through it all the Intelligence Community has often and regularly sounded the domestic and international alarm by bemoaning the fact that no laws adequately protect the sources and methods of the very information they must provide to policy-makers as their eyes and ears abroad. While the Intelligence Community has continued to muddle through most of these problems in one way or another, it seems logical to conclude that the many organizational and legal problems which now confront the producers of intelligence certainly have at least the potential to become magnified in the coming years. Considering the fact that each proposed solution, be it through legislation or otherwise, is not without its own peculiar societal costs, it seems dubious that quantum improvements can be wrought. What does seem possible, however, are changes at the margin concerning many of the issues discussed in this study. In the final analysis, America has yet to determine just what kind of Intelligence Community it wants and how much power and authority it should possess. The time for such a decision would appear to be at hand.

NOTES

Chapter II

1. Interview with Mr. Thomas K. Latimer, Staff Director, House Permanent Select Committee on Intelligence, U.S. House of Representatives, The Capitol, Washington, D.C.: 4 October 1978.

2. Cord Meyer, "CIA's Assessment on Iran Erroneous," Baltimore Evening Sun, 17 November 1978, p. 11.

3. Hanson W. Baldwin, "The Future of Intelligence," Strategic Review, Vol. IV, No. 3, Summer 1976, p. 10.

4. William E. Colby, "Intelligence Secrecy and Security in a Free Society," International Security, Fall 1976, p. 3.

5. Richard Burt, "President Criticizes Effort on Crisis Prediction," New York Times, 23 November 1978, p. 1.

6. Abul Kasim Mansur, "The Crisis in Iran: Why the U.S. Ignored a Quarter Century of Warning," Armed Forces Journal International, January 1979, p. 26-33. Jim Hoagland, "Hill Panel Faults Carter, Aides on Broad Failure in Assessing Iran Crisis," Washington Post, 25 January 1979, p. 1. Seymour M. Hersh, "Ex-analyst Says CIA Rejected Warning on Shah," New York Times, 7 January 1979, p. 3.

7. William E. Colby, "An Intelligence Guide to Intelligence," Chicago Tribune, 15 September 1977, p. 10.

8. Harry Howe Ransom, Intelligence and National Security (Cambridge: Harvard University Press, 1958). Lyman B. Kirkpatrick, Jr., The U.S. Intelligence Community: Foreign Policy and Domestic Activity (New York: Hill and Wang, 1973). Anne Karelekas, History of the Central Intelligence Agency (Laguna Hills, Calif.: Aegean Park Press, 1977).

9. Central Intelligence Agnecy, Fact Book (Washington: CIA Office of Public Affairs, n.d.), (Hereafter referred to as CIA, Office of Public Affairs Packet).

10. U.S. Joint Chiefs of Staff, Dictionary of Military and Associate Terms, Publication No. 1 (Washington: 1974), p. 176.

11. Aaron Wildavsky, The Politics of the Budgetary Process (Boston, Mass.: Little, Brown and Co., 1964), p. 1-5.

12. Dr. James H. Babcock, "Intelligence and National Security," Signal, Vol. 33, No. 3, November-December 1978, p. 16-19. Harry F. Eustace, "Special Report: Changing Intelligence Priorities," Electronic Warfare/Defense Electronics, November 1978, p. 35-37.

13. David Wise, "Is Anybody Watching the CIA?" Inquiry, 27 November 1978, p. 17-21.

14. CIA, Office of Public Affairs Packet.

15. U.S., President, Executive Order 12036, "United States Intelligence Activities," Federal Register 43, no. 18, 26 January 1978, section 1-8, p. 3680. (Hereafter referred to as E.O. 12036).

16. Ibid., Sections 1-9 and 1-10, p. 3681.

17. Ibid., Section 1-11, p. 3681.

18. Ibid., Section 1-14, p. 3684.

19. David Binder, "CIA Head Accused of Tailoring Estimates to Policy; He Denis It," New York Times, 6 November 1978, p. 4.

20. The definitions discussed in this part of the paper are based on an unclassified document tentatively titled, "Defining Intelligence," 5 December 1975, which the author contributed to while assigned to the Defense Intelligence Agency.

21. E. O. 12036, Sec. 1-6, p. 3679.

22. Ibid., Section 1-11, p. 3681.

23. Dr. Gerald P. Dineen, "C^3I: An Interview," Signal, Vol. 33, No. 3., November/December 1978, p. 10-12.

24. Wallace D. Henderson, "Surveillance and Warning," Signal, Vol. 33, No. 3, November/December 1978, p. 39.

Chapter III

1. U.S. Congress, House, Permanent Select Committee on Intelligence, Subcommittee on Evaluation, Iran: Evaluation of U.S. Intelligence Performance Prior to November 1978, Staff Report (Washington: U.S. Govt. Print. Off., 1979) p. 1.

2. Senator Malcom Wallop, quoted in "The U.S. Intelligence Problem," Wall Street Journal, 23 February 1979, p. 16.

3. E. O. 12036, Section 1-1, p. 3675.

4. Ibid, Preamble, p. 3674.

5. Ibid., Section 1-2, p. 3675.

6. Wildavsky, p. 1-5.

7. Eustace, p. 37.

8. E. O. 12036, Section 1-5, p. 3677.

9. Benjamin F. Schemmer, "The Slow Murder of the American Intelligence Community," Armed Forces Journal International, March 1979, p. 52.

10. Babcock, p. 17.

11. CIA Office of Public Affairs.

12. Ibid.

13. Babcock, p. 17.

14. E. O. 12036, Section 1-6, p. 3679.

15. Binder, "CIA Head Accused," p. 4-5.

16. Ibid., p. 4.

17. Schemmer, p. 52.

18. Ibid., p. 53.

19. William R. Van Cleave and Seymour Weiss, "National Intelligence and the U.S.S.R.," National Review, 23 June 1978.

20. Schemmer, p. 53.

Chapter IV

1. U.S. Congress, Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Foreign and Military Intelligence, Final Report, Book I, Senate Report 94-755 (Washington: U.S. Govt. Print. Off., 1976).

2. U.S. Congress, Senate, Senate Resolution 400, Reports 94-675 and 94-770 (Washington: n.p., 19 May 1976); and U.S. Congress, House House Resolution 658, Report 95-498 (Washington: n.p., 14 July 1977).

3. David Wise, "Intelligence Reforms: Less Than Half a Loaf," Washington Post, 23 April 1978, p. D3-5.

4. William R. Corson, The Armies of Ignorance, (New York: Dial Press, 1977), p. 453.

5. U.S. Congress, Senate, Select Committee on Intelligence, Annual Report to the Senate, Senate Report 95-217 (Washington: U.S. Govt. Print. Office, 18 May 1977), p. 1.

6. Letter from Senator Birch Bayh to Warren H. Milberg, 4 April 1979.

7. Corson, p. 454.

8. Ibid., p. 455.

9. U.S. Congress, Senate, A Bill to Improve the Intelligence System of the United States by the Establishment of a Statutory Basis for the National Intelligence Activities of the United States, and for Other Purposes, S. 2525 (Washington: Committee Print, 9 February 1978).

10. Nicholas M. Horrock, "Senate Panel Offers Legislation to Curb Intelligence Agents," New York Times, 10 February 1978, p. 1.

11. "Intelligence Failure #2525, Wall Street Journal, 18 January 1979, p. 11.

12. George Lardner, Jr., "Congress Bypasses Curbs on Spies: Charter Plan is Amended," Providence Sunday Journal, 11 May 1980, p. C1.

13. David M. Alpern, "Unshackling the CIA," Newsweek, 28 January 1980, p. 31-32.

14. Jerry J. Berman, Morton H. Halperin, and John H. F. Shattuck, "Protecting the Names of Intelligence Agents and the Need for a New Charter," First Principles, Vol. 5, No. 5, January-February 1980, p. 4.

15. U.S. Laws, Statutes, etc., "Central Intelligence Agency," U.S. Code, Title I -- Coordination for National Security (Washington: U.S. Govt. Print. Off., 1947), sec. 403 (d)(3).

16. Bill Richards, "Sen. Biden Says U.S. Lost an Entire Spy Network," Washington Post, 13 January 1978, p. 10.

17. James Coates, "U.S. Spies are in a Can of Worms," Chicago Tribune, 15 February 1979, p. 8.

18. U.S. Congress, Senate, Select Committee on Intelligence, Subcommittee on Secrecy and Disclosure, National Security Secrets and the Administration of Justice, Report (Washington: U.S. Govt. Print. Off., 1978). (Hereafter referred to as National Security Secrets.)

Chapter V

1. Colby, "Intelligence Secrecy," p. 2.

2. Report to the President by the Commission on the Organization of the Government for the Conduct of Foreign Policy, Robert D. Murphy, Chairman (Washington: 1975), p. 91. (Hereafter referred to as the Murphy Commission.)

3. U.S. Department of the Air Force, How Intelligence is Used, Supplement to the Air Force Policy Letter for Commanders, No. 4-1976, AFRP 190-2 (Washington: 1976), p. 33.

4. Stansfield Turner, "Saving CIA Secrecy," Christian Science Monitor, 15 November 1978, p. 27.

5. Stansfield Turner, "Freedom Depends on Snoops," Los Angeles Times, 11 September 1978, p. 7.

6. Colby, "Intelligence Secrecy," p. 4.

7. Melvin R. Laird, "Lets Stop Undermining the CIA," Readers Digest, May 1976, p. 37.

8. David Binder, "CIA Aide Says News Leaks in U.S. Worry Allies," New York Times, 18 June 1979, p. 11.

9. Ibid.

10. Nicholas M. Horrock, "White House Reported Acting to Stem Information Leaks," New York Times, 14 May 1978, p. 1.

11. U.S. Congress, Senate, Select Committee on Intelligence, Subcommittee on Legislation, Espionage Laws and Leaks, Hearing (Washington: U.S. Govt. Print. Off., 1979), p. 164-169. (Hereafter referred to as Espionage Laws and Leaks.)

12. Ibid., p. 141.

13. Senator Jake Garn, "Leaks of Top Secret Material 'Reprehensible'," Washington Post, 11 April 1979, p. 18.

14. David Wise, "The New Secrecy," Inquiry, 16 October 1978, p. 20.

15. "Espionage Laws and Leaks," p. 161.

16. Joseph E. Perisco, "The Man Who Sells Broken Secrets," Washington Post (Parade), 8 October 1978, p. 4.

17. Rowland Evans and Robert Novak, "Leaks of Official Secrets Out of Control," Providence Journal, 9 May 1980, p. A18.

18. David M. Alpern, "Unshackling the CIA," Newsweek, 28 January 1980, p. 31-32.

19. Morton H. Halperin, "CIA: What About the Hughes-Ryan Amendment?" First Principles, Vol. 5, No. 5., January-February 1980, p. 18.

20. Charles R. Babcock, "CIA Chief, At National Press Club, Cautions on Intelligence Disclosures," Washington Post, 26 October 1978, p. 2.

21. Murphy Commission, p. 246.

22. George Lardner, Jr., "Changing Climate May Stymie Intelligence Agency Bill," Washington Post, 10 July 1978, p. A2.

23. Ernest W. LeFever and Roy Godson, The CIA and the American Ethic (Washington, D.C.: Georgetown University, 1979), p. 53-59; and the Murphy Commission, Chapter 7.

24. Halperin, p. 18.

25. Charles Mohr, "Aspin Bill Provides Tighter CIA Rein," New York Times, 17 March 1980, p. 13.

26. Edwin Warner, "Strengthening the CIA," Time, 30 April 1979, p. 95-96; and Colby, "Intelligence Secrecy," p. 5-9.

27. Alpern, p. 31.

28. Lardner, "Changing Climate," p. A2.

29. Colby, "Intelligence Secrecy," p. 5.

30. Coates, "U.S. Spies," p. 8.

31. "Press Group Urges Senate to Keep Information Act Provisions for CIA," Providence Journal, 17 Arpil 1980, p. A11.

32. Christine Marwick, "Freeing Intelligence From Freedom of Information: Why?" First Principles, Vol. 5, No. 5., January-February 1980, p. 1, 6-8.

33. Warner, "Strengthening," p. 96.

34. Alpern, p. 31-32.

35. Ibid., p. 32.

36. Perisco, p. 4.

37. Ibid., p. 4-5.

38. "Espionage Laws and Leaks," p. 192-193.

39. "The National Intelligence Act of 1980 (HR 6588)," Congressional Record, 25 February 1980, p. H124.

40. Marwick, p. 7.

41. Warrne Weaver, Jr., "U.S. Information Act: Difficulties Despite Successes," New York Times, 8 August 1977, p. 1.

42. John Stockwell, "A Call for Openness as an Antidote to the CIA's Secrecy ('Poison'), New York Times, 17 May 1978, p. A23.

43. Warner, p. 96.

44. Binder, "News Leaks," p. 11.

45. U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Separation of Powers, The Withholding of Information by the Executive, Hearing (Washington: U.S. Govt. Print. Off., 1971), p. 620.

46. U.S. President, Executive Order 12065, "National Security Information," Office of the White House Press Secretary, 29 June 1978.

47. Bernard D. Nossiter, "GAO Finds 'Secret' Stamp Widely Used," Washington Post, 12 March 1979, p. 1.

48. Stockwell, p. A23.

49. "Espionage Laws and Leaks," p. 256.

50. Turner, "Freedom," p. 7.

51. "Espionage Laws and Leaks," p.3.

52. U.S. President, Fact Sheet, "The New Executive Order on the Security Classification System," Office of the White House Press Secretary, 29 June 1978, p. 1-4.

53. "Too Much is 'Secret' GAO Says," Air Force Times, 19 November 1979, p. 4.

54. U.S. Congress, Comptroller General, Report to the Congress of the United States, Continuing Problems in DoD's Classification of National Security Information, Report LCD 80-16 (Washington: General Accounting Office, 26 October 1979), p. i-iii.

55. "Espionage Laws and Leaks," p. 190.

56. Ibid., p. 190-191.

57. Seymour M. Hersh, "Saigon Flight Held 'Disgrace' to CIA," New York Times, 18 November 1977, p. A22.

58. "Espionage Laws and Leaks," p. 139.

59. Binder, "News Leaks," p. 11.

Chapter VI

1. Letter from William E. Colby to LTCOL Warren H. Milberg, USAF, 9 May 1980.

2. Horrock, "White House," p. 1.

3. Report to the President by the Commission on CIA Activities Within the United States, by Nelson A. Rockefeller, Chairman (Washington: U.S. Govt. Print. Off., 1975), p. 48-53. (Hereafter referred to as Rockefeller Commission.)

4. Rockefeller Commission, p. 48.

5. Corson, p. 427.

6. Rockefeller Commission, p. 56.

7. "Espionage Laws and Leaks," p. 34.

8. U.S. Congress, Senate, Select Committee on Intelligence, Subcommittee on Secrecy and Disclosure, Report on National Security Secrets and the Administration of Justice (Washington: U.S. Govt. Print. Off., 1978), p. 7-8. (Hereafter referred to as "National Security Secrets.")

9. "Espionage Laws and Leaks," p. 124.

10. Melinda Beck, "A Spy Out in the Cold," Newsweek, 28 January 1980, p. 32; and Howard Sibler, "U.S. Trying to Assess Theft of Satellite Data," Omaha World Herald, 30 September 1978, p. 1.

11. Edward Schumacher, "New CIA Secrecy Irritates Diplomats, Scholars," Philadelphia Inquirer, 18 December 1977, p. 7.

12. Anthony Lewis, "The Secrecy Disease," New York Times, 31 October 1977, p. 29.

13. "National Security Secrets," p. 8.

14. Rockefeller Commission, p. 56.

15. "Espionage Laws and Leaks," p. 249.

16. "National Security Secrets," p. 1.

17. Ibid., p. 8.

18. Horrock, "White House," p. 1.

19. "National Security Secrets," p. 8.

20. Coates, "U.S. Spies," p. 8.

21. James Coates, "More Damage than Justice in Espionage Trials," Chicago Tribune, 22 October 1978, p. 8.

22. Anthony Marro, "Panel Says Laws Hinder Security Leak Prosecutions," Washington Star, 11 October 1978, p. 4.

23. "Esiponage Laws and Leaks, p. 51-52.

24. "National Security Secrets," p. 10.

25. U.S. Congress, House, Permanent Select Committee on Intelligence, Classified Information Criminal Trial Procedures Act, S. Report 96-831 to accompany H.R. 4736 (Washington: Committee Print, 18 March 1980), p. 7. (Hereafter referred to as "Classified Procedures Act.")

26. "Espionage Laws and Leaks," p. 202.

27. "Classified Procedures Act," p. 6.

28. U.S. Congress, House, Permanent Select Committee on Intelligence, Subcommittee on Legislation, Graymail Legislation, Hearings (Washington: U.S. Govt. Print. Off., 1979), p. 4-5. (Hereafter referred to as "Graymail Legislation.")

29. "National Security Secrets," p.3 .

30. Ibid., p. 13-16.

31. Ibid., p. 12.

32. Ibid., p. 9.

33. "Espionage Laws and Leaks," p. 157.

34. "Graymail Legislation," p. 113, 36-37.

35. "Classified Procedures Act," p. 9.

36. "Espionage Laws and Leaks," p. 203.

37. "National Security Secrets," p. 21-23.

38. Peter S. Prescott, "How Free to Speak?" Newsweek, 10 March 1980, p. 94-95.

39. Corson, p. 477-478.

40. "National Security Secrets," p. 17.

41. "Espionage Laws and Leaks," p. 94-95.

42. Harold Edgar and Benno C. Schmidt, Jr., "The Espionage Statutues and Publication of Defense Information," Columbia Law Review, Vol. 73, No. 5, May 1973, p. 1076.

43. "Espionage Laws and Leaks," p. 109-116.

44. "National Security Secrets," p. 22.

45. Ibid., p. 25.

46. Seymour M. Hersh, "CIA Analyst Forced Out for Giving Senator Secret Data," New York Times, 13 November 1978, p. 3.

47. "Espionage Laws and Leaks," p. 59-69.

48. Griffin B. Bell, "Secrecy After the Snepp Case," Washington Post, 9 April 1980, p. A21.

49. "Carter Aides Draft Secrecy Rules Shift," New York Times, 15 September 1977, p. 18.

50. Theodore J. Jacobs, "The CIA Needs More than Glue," Washington Post, 15 April 1980, p. A17.

BIBLIOGRAPHY

Alpern, David M. "Unshackling the CIA." Newsweek, 28 January 1980, p. 31-32.

Babcock, Charles R. "CIA Chief, At National Press Club, Cautions on Intelligence Disclosures." Washington Post, 26 October 1978, p. 2.

Babcock, Dr. James H. "Intelligence and National Security." Signal, Vol. 33, No. 3., November-December 1978, p. 16-19.

Beck, Melinda. "A Spy Out in the Cold." Newsweek, 28 January 1980, p. 32.

Bell, Griffin B. "Secrecy After the Snepp Case." Washington Post, 9 April 1980, p. A21.

Berman, Jerry J., Halperin, Morton H., and Shattuck, John H.F. "Protecting the Names of Intelligence Agents and the Need for a New Charter." First Principles, Vol. 5, No. 5, January-February 1980, p. 1-5.

Binder, David. "CIA Aide Says News Leaks in U.S. Worry Allies." New York Times, 18 June 1979, p. 11.

_____. "CIA Head Accused of Tailoring Estimates to Policy; He Denies It." New York Times, 6 November 1978, p. 4.

Burt, Richard. "President Criticizes Error on Crisis Prediction." New York Times, 23 November 1978, p. 1.

"Carter Aides Draft Secrecy Rules Shift." New York Times, 15 September 1977, p. 18.

Coates, James. "More Damge Than Justice in Espionage Trials." Chicago Tribune, 22 October 1978, p. 8.

_____. "U.S. Spies are in a Can of Worms." Chicago Tribune, 15 February 1979, p. 8.

Colby, William E. "An Intelligent Guide to Intelligence." Chicago Tribune, 15 September 1977, p. 10.

_____. "Intelligence Secrecy and Security in a Free Society." International Security, No. 191, Fall 1976, p. 3.

Corson, William R. The Armies of Ignorance. New York: Dial Press, 1977.

"Defining Intelligence." Unpublished document of the Defense Intelligence Agency, 5 December 1975.

Dineen, Dr. Gerald. P. "C^3I: An Interview." Signal, Vol. 33, No. 3, November-December 1978, p. 10-12.

Edgar, Harold and Schmidt, Benno C., Jr. "The Espionage Statutes and Publication of Defense Information." Columbia Law Review, Vol. 73, No. 5, May 1973, p. 929-1080.

Eustace, Harry F. "Special Report: Changing Intelligence Priorities." Electronic Warfare/Defense Electronics, November 1978, p. 35-37.

Evans, Rowland and Novak, Robert. "Leaks of Official Secrets Out of Control." Providence Journal, 9 May 1980, p. 18.

Garn, Senator Jake. "Leaks of Top Secret Material 'Reprehensible'." Washington Post, 11 April 1979, p. 18.

Halperin, Morton H. "CIA: What About the Hughes-Ryan Amendment?" First Principles, Vol. 5, No. 5, January-February 1980, p. 18-20.

Henderson, Wallace D. "Surveillance and Warning." Signal, Vol. 33, No. 3., November-December 1978, p. 39.

Hersh, Seymour M. "CIA Analyst Forced Out for Giving Senator Secret Data." New York Times, 13 November 1978, p. 3.

_____. "Ex-Analyst Says CIA Rejected Warning on Shah." New York Times, 7 January 1979, p. 3.

_____. "Saigon Flight Held 'Disgrace' to CIA." New York Times, 18 November 1977, p. A22.

Honaglan, Jim. "Hill Panel Faults Carter, Aides on Broad Failure in Assessing Iran Crisis." Washington Post, 25 January 1979, p. 1.

Horrock, Nicholas M. "Senate Panel Offers Legislation to Curb Intelligence Agents." New York Times, 10 February 1978, p. 1.

_____. "White House Reported Acting to Stem Information Leaks." New York Times, 14 May 1978, p. 1.

"Intelligence Failure #2525." Wall Street Journal, 18 January 1979, p. 11.

Interview with Thomas K. Latimer, Staff Director, House Permanent Select Committee on Intelligence, U.S. House of Representatives. The Capitol, Washington, D.C.: 4 October 1978.

Jacobs, Theodore J. "The CIA Needs More than Glue." Washington Post, 15 April 1980, p. A17.

Karelekas, Anne. History of the Central Intelligence Agency. Laguna Hills, Calif.: Aegean Park Press, 1977.

Kirkpatrick, Lyman B., Jr. The U.S. Intelligence Community: Foreign Policy and Domestic Activity. New York: Hill and Wang, 1973.

Laird, Melvin R. "Let's Stop Undermining the CIA." Reader's Digest, May 1976, p. 37.

Lardner, George Jr. "Changing Climate May Stymie Intelligence Agency Bill." Washington Post, 10 July 1978, p. A2.

_____. "Congress Bypasses Curb on Spies: Charter Plan is Amended." Providence Sunday Journal, 11 May 1980, p. C1.

LeFever, Ernest W. and Godson, Roy. The CIA and the American Ethic. Washington: Georgetown University Press, 1979.

Letter from Senator Birch Bayh to Warren H. Milberg, 4 April 1979.

Letter from William E. Colby to LTCOL Warren H. Milberg, USAF, 9 May 1980.

Lewis, Anthony. "The CIA is Worried About its New Leaks." New York Times, 4 October 1977, p. E4.

_____. "The Secrecy Disease." New York Times, 31 October 1977, p. 29.

Mansur, Abul Kasim. "The Crisis in Iran: Why the U.S. Ignored a Quarter Century of Warning." Armed Forces Journal International, January 1979, p. 26-33.

Marro, Anthony. "Panel Says Laws Hinder Security Leak Prosecutions." Washington Star, 11 October 1978, p. 4.

Marwick, Christine. "Freeing Intelligence From Freedom of Information: Why?" First Principles, Vol. 5, No. 5, January-February 1980, p. 1, 6-8.

Meyer, Cord. "CIA's Assessment on Iran Erroneous." Baltimore Evening Sun, 17 November 1978, p. 11.

Mohr, Charles. "Aspin Bill Provides Tighter CIA Rein." New York Times, 17 March 1980, p. 13.

Mossiter, Bernard D. "GAO Finds 'Secret' Stamp Widely Used." Washington Post, 12 March 1979, p. 1.

Perisco, Joseph E. "The Man Who Sells Broken Secrets." Washington Post, 8 October 1978, p. 4. (Parade.)

"Press Group Urges Senate to Keep Information Act Provisions for CIA." Providence Journal, 17 April 1980, p. All.

Prescott, Peter S. "How Free to Speak?" Newsweek, 10 March 1980, p. 94-95.

Ransom, Harry Howe. Intelligence and National Security. Cambridge: Harvard University Press, 1958.

Report to the President by the Commission on CIA Activities Within the United States. Nelson A. Rockefeller, Chairman. Washington: U.S. Govt. Print. Off., 1975.

Report to the President by the Commission on the Organization of the Government for the Conduct of Foreign Policy. Robert D. Murphy, Chairman. Washington: U.S. Govt. Print. Off., 1975.

Richards, Bill. "Sen. Biden Says U.S. Lost an Entire Spy Network." Washington Post, 13 January 1978, p. 10.

Schemmer, Benjamin F. "The Slow Murder of the American Intelligence Community." Armed Forces Journal International, March 1979, p. 52.

Schumacker, Edward. "New CIA Secrecy Irritates Diplomats, Scholars." Philadelphia Inquirer, 18 December 1977, p. 7.

Silber, Howard. "U.S. Trying to Assess Theft of Satellite Data." Omaha World Herald, 30 September 1978, p. 1.

Stockwell, John. "A Call for Openness as an Antidote to the CIA's Secrecy ('Poison')." New York Times, 17 Mary 1978, p. A23.

"The National Intelligence Act of 1980 (H.R. 6588)." Congressional Record, 25 February 1980, p. H124.

"Too Much is 'Secret' GAO Says." Air Force Times, 19 November 1979, p. 4.

Turner, Stansfield, "Freedom Depends on Snoops." Los Angeles Times, 11 September 1978, p. 7.

_____. "The CIA's 'Unequivocal' Right to Prior Review." Washington Post, 7 December 1977, p. 27.

_____. "Saving CIA Secrecy." Christian Science Monitor, 15 November 1978, p. 27.

U.S. Congress. Comptroller General. Continuing Problems in DoD's Classification of National Security Information. Report LCD 80-16. Washington: General Accounting Office, 26 October 1979.

_____. House. House Resolution 658. Report No. 95-498. Washington: Committee Print, 14 July 1977.

_____. _____. Permanent Select Committee on Intelligence. Classified Information to Accompany Criminal Trial Procedures Act. Senate Report 96-831 to accompany H.R. 4736. Washington: U.S. Govt. Print. Off., 18 March 1980.

_____. _____. _____. Subcommittee on Evaluation. Iran: Evaluation of U.S. Intelligence Performance Prior to November 1978. Staff Report. Washington: U.S. Govt. Print. Off., 1979.

_____. _____. _____. Subcommittee on Legislation. Espionage Laws and Leaks. Hearing. Washington: U.S. Gwvt. Print. Off., 1979.

_____. _____. _____. _____. Graymail Legislation. Hearing. Washington: U.S. Govt. Print. Off., 20 September 1979.

_____. _____. _____. _____. Impact of the Freedom of Information Act and Privacy Act on Intelligence Activities. Hearing. Washington: U.S. Govt. Print. Off., 5 April 1979.

_____. Seante. A Bill to Improve the Intelligence System of the United States by the Establishment of a Statutory Basis for the National Intelligence Activities of the United States, and for Other Purposes. Senate Bill 2525. Washington: Committee Print, 9 February 1978.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Separation of Powers. Executive Privilege: The Withholding of Information by the Executive. Hearing. Washington: U.S. Govt. Print. Off., 1961.

_____. _____. Select Committee on Intelligence. Annual Report to the Senate. Report No. 95-217. Washington: n.p., 18 May 1977.

_____. _____. _____. Subcommittee on Secrecy and Disclosure. National Security Secrets and the Administration of Justice. Report. Washington: U.S. Govt. Print. Off., 1978.

_____. _____. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Foreign and Military Intelligence. Final Report, Book I, Sen. Rept. 94-755. Washington: U.S. Govt. Print. Off., 1976.

_____. _____. Senate Resolution 400. Reports 94-675 and 94-770. Washington: n.p., 19 May 1976.

U.S. Department of the Air Force. How Intelligence is Used. Supplement to the Air Force Policy Letter for Commanders, No. 4-1976. AFRP. 190-2. Washington: n.p. 1976.

"U.S. Intelligence Problem, The," Wall Street Journal 23 February 1979, p. 16.

U.S. Joint Chiefs of Staff. Dictionary of Military and Associated Terms. Publication No. 1. Washington: U.S. Govt. Print. Off., 3 September 1974.

U.S. Laws, Statutes, etc. U.S. Code, Title I -- Coordination for National Security. Washington: U.S. Govt. Print. Off., 1947.

U.S. President. Executive Order 12065. "National Security Information." Office of the White House Press Secretary, 29 June 1978.

_____. Executive Order 12036. "United States Intelligence Activities." Federal Register 43, No. 18, 26 January 1978, p. 3674-3692.

_____. Fact Sheet. "The New Executive Order on the Security Classification System." Office of the White House Press Secretary, 29 June 1978, p. 1-4.

Van Clave, William R. and Weiss, Seymour. "National Intelligence and the U.S.S.R." National Review,, 23 June 1978, p. 11.

Warner, Edwin. "Strengthening the CIA." Time, 30 April 1979, p. 95-96.

Weaver, Warren, Jr. "U.S. Information Act: Difficulties Despite Successes." New York Times, 8 August 1977, p. 1.

Wildavsky, Aaron. The Politics of the Budgetary Process. Boston: Little, Brown, 1964.

Wise, David. "Intelligence Reforms: Less Than Half a Loaf." Washington Post, 23 April 1978, p. D3-5.

_____. "Is Anybody Watching the CIA?" Inquiry, 27 November 1978, p. 17-21.

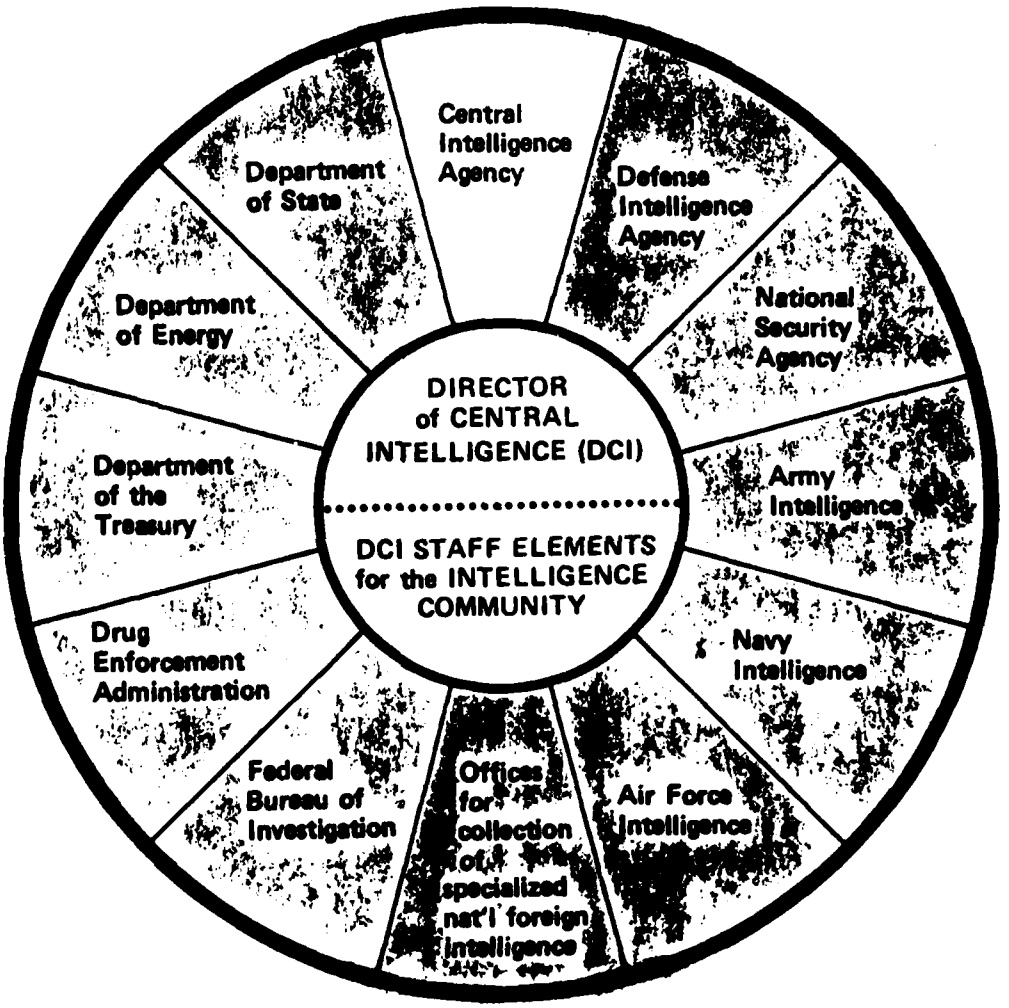
_____. "The New Secrecy." Inquiry, 16 October 1978, p. 20-23.

APPENDIX I

THE U.S. INTELLIGENCE COMMUNITY

APPENDIX I

The Intelligence Community



Source: Central Intelligence Agency "Fact Book," published by CIA Office of Public Affairs.

CENTRAL INTELLIGENCE AGENCY

Intelligence is knowledge and foreknowledge of the world around us—the prelude to Presidential decision and action.

WASHINGTON, D.C. 20505

PUBLIC AFFAIRS
Phone: (703) 351-7676

The Intelligence Cycle

is the process by which information is acquired, converted into intelligence, and made available to policymakers. There are usually five steps which constitute *The Intelligence Cycle.*

1. Planning and Direction

This involves the management of the entire intelligence effort, from the identification of the need for data to the final delivery of an intelligence product to a customer.

The whole process is initiated by requests or requirements for intelligence on certain subjects. These are based on the ultimate needs of the policymakers—the President, the National Security Council, and other major departments and agencies of government.

2. Collection

This involves the gathering of the raw data from which finished intelligence will be produced. There are many sources for the collection of information, including foreign radiobroadcasts, newspapers, periodicals, and official government personnel stationed in American embassies abroad.

There are also secret sources, such as agents and defectors who provide information obtainable in no other way.

Finally, technical collection—photography and electronics—has come to play an indispensable part in modern intelligence by extending the Nation's sensory system—its eyes and ears.

3. Processing

This step is concerned with the conversion of the vast amount of information coming into the system to a form more suitable for the production of finished intelligence, such as in language translations, decryption, and sorting by subject matter. The information that does not go directly to analysts is sorted and made available for rapid computer retrieval.

Processing also refers to data reduction—interpretation of the information stored on film and tape through the use of highly refined photographic and electronic processes.

4. Production and Analysis

This refers to the conversion of basic information into finished intelligence. It includes the integration, evaluation, and analysis of all available data and the preparation of a variety of intelligence products. Such products or estimates may be presented as briefings, brief reports or lengthy studies.

The "raw intelligence" collected is frequently fragmentary and at times contradictory. Analysts, who are subject-matter specialists for a particular country, produce finished intelligence by evaluating and integrating the various pieces of data and interpreting their meaning and significance.

The subjects involved may concern different regions, problems, or personalities in various contexts—political, geographic, economic, military, scientific, or biographic. Current events, capabilities, or probable developments in the future may also be examined.

5. Dissemination

The last step is the distribution and handling of the finished intelligence to the consumers of intelligence, the same policymakers whose needs triggered the Intelligence Cycle.

Sound policy decisions must be based on sound knowledge. Intelligence aims to provide that knowledge.

CENTRAL INTELLIGENCE AGENCY

WASHINGTON, D.C. 20505

PUBLIC AFFAIRS
Phone: (703) 351-7676

THE PRESIDENT'S INTELLIGENCE ORGANIZATION

Presidential Executive Order No. 12036, 26 January 1978, assigns the Director of Central Intelligence the responsibility to act as the primary adviser to the President and the National Security Council on national foreign intelligence. To discharge this and other assigned duties, the Director is the appointed head of both the Central Intelligence Agency and the Intelligence Community. These relationships and the mechanisms established by the Executive Order to sustain them are discussed below.

NATIONAL SECURITY COUNCIL (NSC)

The NSC was established by the National Security Act of 1947 to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security. The NSC is the highest Executive Branch entity providing review of, guidance for, and direction to the conduct of all national foreign intelligence and counterintelligence activities. The statutory members of the NSC are the President, Vice President, the Secretary of State, and the Secretary of Defense. The Director of Central Intelligence and the Chairman of the Joint Chiefs of Staff participate as advisers.

POLICY REVIEW COMMITTEE (PRC)

This committee of the NSC is composed of the Vice President; the Secretaries of State, Treasury, and Defense; the Assistant to the President for National Security Affairs; the Chairman of the Joint Chiefs of Staff; the Director of Central Intelligence; and other senior officials as appropriate. The PRC Chairman varies according to the meeting agenda; e.g., the Director of Central Intelligence is chairman when the body addresses intelligence matters. PRC duties in connection with national foreign intelligence require that it establish requirements and priorities, relate these requirements to budget proposals and resource allocations, review and evaluate the quality of intelligence products, and report annually on its activities to the NSC.

SPECIAL COORDINATION COMMITTEE (SCC)

This committee of the NSC is chaired by the Assistant to the President for National Security Affairs and is composed of the statutory members of the NSC and other senior officials as appropriate. The SCC deals with cross-cutting

issues requiring coordination in the development of options and the implementation of Presidential decisions. Regarding intelligence issues, the SCC is required to consider and submit to the President policy recommendations on special activities; review and approve proposals for sensitive foreign intelligence collection operations; develop policy, standards, and doctrine for and approve U.S. counterintelligence activities; and submit annually to the President an assessment of the relative threat to U.S. interests from intelligence and security services of foreign powers and from international terrorist activities.

INTELLIGENCE OVERSIGHT BOARD (IOB)

The President's Intelligence Oversight Board functions within the White House. The IOB consists of three members from outside the government who are appointed by the President. The duties of the IOB include reviewing the practices and procedures of the Inspectors General and General Counsels with responsibilities for agencies within the Intelligence Community, for discovering and reporting to the IOB intelligence activities that raise questions of legality or propriety, reporting to the President any intelligence activities that raise serious questions of legality, and forwarding to the Attorney General reports on activities that raise questions of legality.

THE INTELLIGENCE COMMUNITY

While the Director of Central Intelligence is head of the CIA, he is at the same time leader of the Intelligence Community of which CIA is but one component. The Intelligence Community refers in the aggregate to those Executive Branch agencies and organizations that conduct the variety of intelligence activities which comprise the total U.S. national intelligence effort. The Community includes the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; offices within the Department of Defense for collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the military services, the Federal Bureau of Investigation, the Department of the Treasury, the Department of Energy, and the Drug Enforcement Administration; and staff elements of the Office of the Director of Central Intelligence. Members of the Intelligence Community advise the Director of Central Intelligence through their representation on a number of specialized committees that deal with intelligence matters of common concern. Chief among these groups is the National Foreign Intelligence Board which the Director chairs and which includes as an observer a representative of the Assistant to the President for National Security Affairs.

APPENDIX II

EXTRACT FROM THE NATIONAL SECURITY ACT OF 1947

APPENDIX II

National Security Act of 1947, as amended

Title 1—Coordination for National Security

NATIONAL SECURITY COUNCIL

SECTION 101. (a) There is established a council to be known as the National Security Council (hereinafter in this section referred to as the "Council").

The President of the United States shall preside over meetings of the Council: *Provided*, That in his absence he may designate a member of the Council to preside in his place.

The function of the Council shall be to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security.

The Council shall be composed of—

(1) the President;

(2) the Vice President;

(3) the Secretary of State;

(4) the Secretary of Defense;

(5) the Director for Mutual Security [now abolished];

(6) the Chairman of the National Security Resources Board [now abolished];

(7) the Secretaries and Under Secretaries of other executive departments and of the military departments, the Chairman of the Munitions Board [now abolished]; and the Chairman of the Research and Development Board [now abolished]; when appointed by the President by and with the advice and consent of the Senate, to serve at his pleasure.

Source: Extract from the National Security Act of 1947: Rockefeller Commission Report, p. 275.

CENTRAL INTELLIGENCE AGENCY

SEC. 102. (a) There is established under the National Security Council a Central Intelligence Agency with a Director of Central Intelligence who shall be the head thereof, and with a Deputy Director of Central Intelligence who shall act for, and exercise the powers of, the Director during his absence or disability. The Director and the Deputy Director shall be appointed by the President, by and with the advice and consent of the Senate, from among the commissioned officers of the armed services, whether in an active or retired status, or from among individuals in civilian life: *Provided, however*, That at no time shall the two positions of the Director and Deputy Director be occupied simultaneously by commissioned officers of the armed services, whether in an active or retired status.

(b) (1) If a commissioned officer of the armed services is appointed as Director, or Deputy Director, then—

(A) in the performance of his duties as Director, or Deputy Director, he shall be subject to no supervision, control, restriction, or prohibition (military or otherwise) other than would be operative with respect to him if he were a civilian in no way connected with the Department of the Army, the Department of the Navy, the Department of the Air Force, or the armed services or any component thereof; and

(B) he shall not possess or exercise any supervision, control, powers or functions (other than such as he possesses, or is authorized or directed to exercise, as Director, or Deputy Director) with respect to the armed services or any component thereof, the Department of the Army, Department of the Navy, or the Department of the Air Force, or any branch, bureau, unit, or division thereof, or with respect to any of the personnel (military or civilian) of any of the foregoing.

(2) Except as provided in paragraph (1) of this subsection, the appointment of the office of Director, or Deputy Director, of a commissioned officer of the armed services, and his acceptance of and service in such office, shall in no way affect any status, office, rank, or grade he may occupy or hold in the armed services, or any emolument, perquisite, right privilege, or benefit incident to or arising out of any such status, office, rank, or grade. Any such commissioned officer shall, while serving in the office of Director, or Deputy Director, continue to hold rank and grade not lower than that in which serving at the time of his appointment and to receive the military pay and allowances (active or retired, as the case may be, including personal money allowance) payable to a commissioned officer of his grade and length of service for which the appropriate department shall be reimbursed from any funds available to defray the expenses of the Central Intelligence Agency. He also shall be paid by the Central Intelligence

Agency from such funds an annual compensation at a rate equal to the amount by which the compensation established for such position exceeds the amount of his annual military pay and allowances.

(3) The rank or grade of any such commissioned officer shall, during the period in which such commissioned officer occupies the office of Director of Central Intelligence, or Deputy Director of Central Intelligence, be in addition to the numbers and percentages otherwise authorized and appropriated for the armed service of which he is a member.

(c) Notwithstanding the provisions of section 652 [now 7501] of Title 5, or the provisions of any other law, the Director of Central Intelligence may, in his discretion, terminate the employment of any officer or employee of the Agency whenever he shall deem such termination necessary or advisable in the interests of the United States, but such termination shall not affect the right of such officer or employee to seek or accept employment in any other department or agency of the Government if declared eligible for such employment by the United States Civil Service Commission.

(d) For the purpose of coordinating the intelligence activities of the several Government departments and agencies in the interest of national security, it shall be the duty of the Agency, under the direction of the National Security Council—

(1) to advise the National Security Council in matters concerning such intelligence activities of the Government departments and agencies as relate to national security;

(2) to make recommendations to the National Security Council for the coordination of such intelligence activities of the departments and agencies of the Government as relate to the national security;

(3) to correlate and evaluate intelligence relating to the national security, and provide for the appropriate dissemination of such intelligence within the Government using where appropriate existing agencies and facilities: *Provided*, That the Agency shall have no police, subpoena, law-enforcement powers, or internal-security functions: *Provided further*, That the departments and other agencies of the Government shall continue to collect, evaluate, correlate, and disseminate departmental intelligence: *And provided further*, That the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure;

(4) to perform, for the benefit of the existing intelligence agencies, such additional services of common concern as the National Security Council determines can be more efficiently accomplished centrally;

(5) to perform such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct.

(e) To the extent recommended by the National Security Council and approved by the President, such intelligence of the departments and agencies of the Government, except as hereinafter provided, relating to the national security shall be open to the inspection of the Director of Central Intelligence, and such intelligence as relates to the national security and is possessed by such departments and other agencies of the Government, except as hereinafter provided, shall be made available to the Director of Central Intelligence for correlation, evaluation, and dissemination: *Provided, however*, That upon the written request of the Director of Central Intelligence, the Director of the Federal Bureau of Investigation shall make available to the Director of Central Intelligence such information for correlation, evaluation, and dissemination as may be essential to the national security.

(f) Effective when the Director first appointed under subsection (a) of this section has taken office—

(1) the National Intelligence Authority (11 Fed. Reg. 1337, 1339, February 5, 1946) shall cease to exist; and

(2) the personnel, property, and records of the Central Intelligence Group are transferred to the Central Intelligence Agency, and such Group shall cease to exist. Any unexpended balances of appropriations, allocations, or other funds available or authorized to be made available for such Group shall be available and shall be authorized to be made available in like manner for expenditure by the Agency.

APPENDIX III

THE FEDERAL BUREAU OF INVESTIGATION'S "ELEVEN QUESTIONS"

APPENDIX III

QUESTIONS ASKED BY THE DEPARTMENT OF JUSTICE BEFORE INITIATING A LEAK INVESTIGATION

1. The date and identity of the article or articles disclosing the classified information.

2. Specific statements in the article which are considered classified and whether the data was properly classified.

3. Whether the classified data disclosed is accurate.

4. Whether the data came from a specific document and, if so, the origin of the document and the name of the individual responsible for the security of the classified data disclosed.

5. The extent of official dissemination of the data.

6. Whether the data has been the subject of prior official releases.

7. Whether prior clearance for publication or release of the information was sought from proper authorities.

8. Whether the material or portions thereof or enough background data has been published officially or in the press to make an educated speculation on the matter possible.

9. Whether the data can be declassified for the purpose of prosecution and, if so, the name of the person competent to testify concerning the classification.

10. Whether declassification had been decided upon prior to the publication or release of the data.

11. What effect the disclosure of the classified data could have on the national defense.

Source: FBI "11 Questions," Hearings on "Espionage Laws and Leaks," p. 249.

APPENDIX IV

BRITISH OFFICIAL SECRETS ACT

APPENDIX IV

SECTION 2 OF THE (BRITISH) OFFICIAL SECRETS ACT 1911

Text of section 2 of the 1911 Act (as amended)

"Wrongful communication etc. of information

(1) If any person having in his possession or control any secret official code word, or pass word, or any sketch, plan, model, article, note, document, or information which relates to or is used in a prohibited place or anything in such a place or which has been made or obtained in contravention of this Act, or which has been entrusted in confidence to him by any person holding office under Her Majesty or which he has obtained or to which he has had access owing to his position as a person who holds or has held office under Her Majesty, or as a person who holds or has held a contract made on behalf of Her Majesty or as a person who is or has been employed under a person who holds or has held such an office or contract—

(*a*) communicates the code word, pass word, sketch, plan, model, note, document, or information to any person, other than a person to whom he is authorized to communicate it, or a person to whom it is in the interest of the State his duty to communicate it; or

(*aa*) uses the information in his possession for the benefit of any foreign Power or in any other manner prejudicial to the safety or interests of the State;

(*b*) retains the sketch, plan, model, article, note, or document in his possession or control when he has no right to retain it or when it is contrary to his duty to retain it, or fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof; or

(*c*) fails to take reasonable care of, or so conducts himself as to endanger the safety of the sketch, plan, model, article, note, document, secret official code or pass word or information;

that person shall be guilty of a misdemeanour.

(1A) If any person having in his possession or control any sketch, plan, model, article, note, document, or information which relates to munitions of war, communicates it directly or indirectly to any foreign Power, or in any other manner prejudicial to the safety or interests of the State, that person shall be guilty of a misdemeanour.

(2) If any person receives any secret official code word, or pass word, or sketch, plan, model, article, note, document, or information, knowing, or having reasonable ground to believe, at the time when he receives it, that the code word, pass word, sketch, plan, model, article, note, document, or information is communicated to him in contravention of this Act, he shall be guilty of a misdemeanour, unless he proves that the communication to him of the code word, pass word, sketch, plan, model, article, note, document, or information was contrary to his desire."

Source: British Official Secrets Act: Report on "National Security Secrets," p. 48-57.

*Notes on section 2**

1. The main offence created by section 2 is committed by a person who, "having in his possession any information which he has obtained owing to his position as a person who holds office under Her Majesty or a contract on behalf of Her Majesty", "communicates the information to any person other than a person to whom he is authorised to communicate it". In ordinary language, it is an offence under section 2(1)(a) for a Crown servant or Government contractor to make an unauthorised disclosure of information which he has learnt in the course of his job. The word "communicates" has its ordinary meaning. It covers the passing of a document or other record, and the transmission of information orally. All kinds of information are covered. The section contains a list, several times repeated, which includes code words, sketches, models, etc., but in each case this list ends with the all-embracing words "document or information". There is no limitation of subject matter; but section 2 applies only to "official information", in the sense described in notes 2 and 3.

2. The main class of information covered by section 2(1)(*a*) is defined by reference to two classes of persons. The first class comprises persons "holding office under Her Majesty". This includes not only civil servants and members of the Diplomatic Service, but also Ministers of the Crown, members of the Judiciary (from Judges of the Supreme Court to Justices of the Peace), members of the Armed Forces, police officers (by virtue of their office of constable) and others. By virtue of the definition in section 12 of the 1911 Act it includes any office or employment in or under any department of the Government of the United Kingdom. Employees of the Post Office and of the United Kingdom Atomic Energy Authority are deemed by the Post Office Act 1969 and the Atomic Energy Authority Act 1954 respectively to be holders of an office under Her Majesty for this purpose. The above-mentioned persons are for convenience described as Crown servants in this Report. Whether members and employees of public bodies on the fringes of central Government, and persons appointed by Ministers, are Crown servants for this purpose is in many cases unclear. The second class of persons specified in section 2(1)(*a*) comprises those who hold a contract made on behalf of Her Majesty, and their employees. Former members of both classes are also covered.

3. "Official information", as we use the term in this Report, is information which a Crown servant or Government contractor (in the sense explained in note 2) learns in his capacity as such. The unauthorised communication of such information by such a person is an offence under section 2(1)(*a*). A person who is in neither of these classes also commits an offense under section 2(1)(*a*) if he makes an unauthorised communication of official information which has been entrusted to him in confidence by a Crown servant. The meaning of "entrusted in confidence" is not defined. These words may bring within the scope of section 2(1)(*a*) a wide range of people, for instance those involved in the outside consultations frequently undertaken by central Government, which may be conducted in confidence.

---

*These notes are taken from the report of the Departmental Committee on section 2 of the Official Secrets Act 1911 (the Franks Committee) Cmnd. 5104.

4. Note 3 has described offences under section 2(1)(*a*) committed by those who are properly in possession of official information. It is also an offence under section 2(1)(*a*) to make an unauthorised communication of information "which has been made or obtained in contravention of this Act". Some uncertainty attaches to these words, since nothing in section 2 speaks of its being a contravention of the section to make or obtain anything, whereas section 1(1)(*b*) and (*c*) create offences which use these words. The commonly accepted interpretation, however, is that when official information has been communicated in contravention of section 2, the recipient commits an offence if he in turn communicates that information without authority. This means that it is possible to have a chain of unauthorised communications, each link in the chain committing an offence under section 2(1)(*a*).

5. A Crown servant or Government contractor does not commit an offence under section 2(1)(*a*) if he communicates official information to a "person to whom he is authorised to communicate it, or a person to whom it is in the interest of the State his duty to communicate it". The Act provides no guidance on the interpretation of these words. The way in which they are in practice interpreted by Crown servants is explained in paragraph 18 of the Report. In brief, implicit authorisation to disclose official information is regarded as flowing from the nature of each Crown servant's job. This interpretation can be adapted so as to apply to Government contractors and persons entrusted with official information in confidence. The meaning of the words quoted above in relation to other persons is obscure.

6. Section 2(1)(*a*) is concerned with the communication of official information, and section 2(2) with its receipt. Section 2(2) provides that, where a recipient of official information knows or has reasonable grounds to believe, at the time, that its communication to him constituted a breach of the Official Secrets Act, he is also guilty of an offence unless he proves that the communication to him was "contrary to his desire". It is immaterial whether the recipient makes any use of the information. If he in turn communicates it, he may then commit an offence under section 2(1)(*a*) (see note 4).

7. There are a number of other offences under section 2, less important than those discussed in the notes above.

(*a*) Under section 2(1)(*a*), an offence is committed by a person possessing any secret official code word or pass word, or any information relating to or used in a prohibited place, or anything in such a place, who communicates it without authority. This offence is not restricted to the Crown servants and the other classes of person mentioned in notes 2 and 3. All persons are forbidden to pass on information about prohibited places, however acquired. Prohibited places are defined in *section 3* of the 1911 Act, and include any defence "establishment or station, factory, dockyard, mine, minefield, camp, ship or aircraft belonging to or occupied by or on behalf of Her Majesty or any telegraph, telephone, wireless or signal station or office". The Secretary of State has power to declare other places (such as public utilities) to be prohibited places on the ground that information about them would be useful to an enemy.

(*b*) The other offences created by section 2(1)(*aa*), (1)(*b*), (1)(*c*) and (1A) are relatively straightforward. Subsection (1)(*aa*) and subsection (1A), which were added by the 1920 Act, both include the words "manner prejudicial to the safety or interests of the State", which gives them an affinity with section 1. The offence in subsection (1A), like that relating to prohibited places, can be committed by any person who has information about munitions of war in his possession, however he obtained it.

APPENDIX V

THE ESPIONAGE STATUTES

APPENDIX V

CURRENT STATUTES

50 U.S.C. 783

§ 783. Offenses.

(a) Conspiracy or attempt to establish totalitarian dictatorship.

It shall be unlawful for any person knowingly to combine, conspire, or agree with any other person to perform any act which would substantially contribute to the establishment within the United States of a totalitarian dictatorship, as defined in paragraph (15) of section 782 of this title, the direction and control of which is to be vested in, or exercised by or under the domination or control of, any foreign government, foreign organization, or foreign individual: *Provided, however*, That this subsection shall not apply to the proposal of a constitutional amendment.

(b) Communication of classified information by Government officer or employee.

It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

(c) Receipt of, or attempt to receive, by foreign agent or member of Communist organization, classified information.

It shall be unlawful for any agent or representative of any foreign government, or any officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, knowingly to obtain or receive, or attempt to obtain or receive, directly or indirectly, from any officer or employee of the United States or of any department or agency thereof or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, unless special authorization for such communication shall first have been obtained from the head of the department, agency, or corporation having custody of or control over such information.

(d) Penalties for violation.

Any person who violates any provision of this section shall, upon conviction thereof, be punished by a fine of not more than $10,000, or imprisonment for not more than ten years, or by both such fine and such imprisonment, and shall, moreover, be thereafter ineligible to hold any office, or place of honor, profit, or trust created by the Constitution or laws of the United States.

(e) Limitation period.

Any person may be prosecuted, tried, and punished for any violation of this section at any time within ten years after the commission of such offense, notwithstanding the provisions of any other statute of limitations: *Provided*, That if at the time of the commission of the offense such person is an officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, such person may be prosecuted, tried, and punished for any violation of this section at any time within ten years after such person has ceased to be employed as such officer or employee.

(f) Membership as not violation per se.

Neither the holding of office nor membership in any Communist organization by any person shall constitute per se a violation of subsection (a) or subsection (c) of this section or of any other criminal statute. (Sept. 23, 1950, ch. 1024, title I, § 4, 64 Stat. 991; Jan. 2, 1968, Pub. L. 90-237, § 3, 81 Stat. 765.)

Source: Espionage Laws: Hearings on "Espionage Laws and Leaks," p. 270-272.

18 U.S.C. 793

§ 793. Gathering, transmitting, or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or

transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer —

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

June 25, 1948, c. 645, 62 Stat. 736; Sept. 23, 1950, c. 1024, Title I, § 18, 64 Stat. 1003.

18 U.S.C. 794

§ 794. Gathering or delivering defense information to aid foreign government

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States, or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

June 25, 1948, c. 645, 62 Stat. 737; Sept. 3, 1954, c. 1261, Title II, § 201, 68 Stat. 1219.

18 U.S.C. 798

§ 798. Disclosure of Classified information [1]

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

[1] So enacted. Second section 798 enacted on June 30, 1953, set out below.

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

Added Oct. 31, 1951, c. 655, § 24(a), 65 Stat. 719.

50 U.S.C. 783(b)

Communication of classified Information by Government officer or employee

(b) It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.