INTELLIGENCE MONOGRAPH

SECRECY vs. DISCLOSURE

A STUDY IN SECURITY CLASSIFICATION

CENTER FOR THE STUDY OF INTELLIGENCE

CENTRAL INTELLIGENCE AGENCY

TR/IM 76-06

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

TABLE OF CONTENTS

SECRECY VS. DISCLOSURE - A STUDY IN SECURITY CLASSIFICATION

> "We have an obligation to provide as much information as possible on an unclassified basis, but without derogation of the necessity to protect sensitive sources and methods and to protect information which truly requires sensitive treatment."
>
> Director of Central Intelligence
> *Guiding Principles for the Intelligence Community.*

INTRODUCTION

This Study is the first in a series undertaken by the Center on the subject of compartmentation,[1] the basic purpose of which in the Agency and elsewhere is to preserve secrecy. The principal technique for doing this, the one on which the others repose, is the federal classification system. This Study looks first at the historical development of classification, seeking to isolate its endemic problems and to gain a fresh perspective on a procedure that has become hackneyed for most of us. The Study then focuses on classification practices within CIA--a major factor in Agency compartmentation.

It also looks at the interrelationship of classification and the Freedom of Information and Privacy Acts, at the statutory protection of sources and methods, and at the other legal barriers to the disclosure of foreign intelligence information.* The preservation of secrecy through classification and the other techniques of compartmentation ultimately depends on the legal power to withhold information and to deter unauthorized disclosure.

The protection of classified information in our society has always involved a tug of war between the conflicting requirements of secrecy and publicity. From the earliest days there has been conflict between the Executive and the Legislature over Executive confidentiality. Events, moreover, since the adoption of the present classification system in 1972--particularly Vietnam, Watergate, and various disclosures and investigations--have intensified these historical tensions, generating, both inside and outside the government, sharp

*The author of this Study was [redacted] assisted by the staff and fellows of the Center for the Study of Intelligence. The methodology of the Study involved interviewing key personnel in the Agency involved with classification and related matters and extensive research in the available literature. Congressional hearings and studies are the most important source of the latter. Although there have been numerous studies of codeword compartmentation within CIA and the Intelligence Community, we are not aware of any single, published, comprehensive study of the classification system done within the Intelligence Community. We have, therefore striven for comprehensiveness in the Study both as a means of solving the immediate problems at hand and of facilitating the further research of others concerned with classification.

criticism of classification practices. Whenever classification decisions have lacked an aura of credibility for Congress and the public, the information they protected has been vulnerable to disclosure. No statute or Executive order has long sufficed to protect information that Congress or the public has come to regard as pseudo-secrets or cover-up of illegality. The amended Freedom of Information Act (FOIA) and the Privacy Act have brought the executive branch to the realization that in a democracy the "right to know" of Congress and the public is just as imperious as the "need to know" of the bureaucrat. This counterpoint between secrecy and disclosure and, in a closely related sense, between secrecy and publicity, is the main theme of this Study.

The developments referred to above have led the executive branch to reexamine the full implications of secrecy and classification. National Security Study Memorandum (NSSM) 229, dated 16 August 1975, created an ad hoc interagency group, under the chairmanship of the Deputy Assistant to the President for National Security Affairs, charged with making a comprehensive study of the classification system and submitting, if appropriate, recommendations for the revision of E.O. 11652 and possible legislation on the management of classified information. Symptomatic of CIA concern with classification problems was the establishment on 13 January 1976 of an interagency group chaired by

Dr. Edward Proctor, charged with finding "a basis for designing a simplified classification system which will provide the necessary protection of intelligence sources and methods and will facilitate access to the results of the intelligence process by all consumers who need the intelligence product."* Finally, E.O. 11905, issued 18 February 1976, directed the DCI "to establish a vigorous program to downgrade and declassify foreign intelligence information as appropriate and consistent with E.O. 11652."

The Center hopes that this Study will contribute to the efforts of those officers engaged in carrying out the above orders and will be of use to others interested in the impact of a vital adjunct of the intelligence process within the CIA. A summary of its principal conclusions and recommendations is set forth in the next section. (The full text of the recommendations is contained in the final section.)

*In an effort to provide an independent perspective on classification problems, this Study has not been linked with the results of the Proctor group.

PRINCIPAL CONCLUSIONS AND RECOMMENDATIONS

Throughout the history of the classification system, going back even to its nineteenth century precursors, certain negative traits--overclassification, unnecessary classification, vagueness of the classification criteria, and accumulation of vast quantities of classified paper--have always been present. Unfortunately, they are all part of the classification experience of the CIA today. In recent years, the negative traits have attracted public and congressional attention and have resulted in a series of studies, regulations, and reforms intended to improve the system. There has been some improvement, but not much.

- Although recognizing the primary responsibility of the National Security Council and the ICRC in the area of classification, this Study recommends that CIA take a leading role in the development of classification theory and in the reform of the present classification system. In this sense, six recommendations are offered in the Study for the reform of E.O. 11652.

Their principal thrust is to:

- increase the specificity of the classification criteria,
- prevent misclassification for reasons of administrative privacy,
- replace the ICRC with a greatly strengthened interagency classification board,
- restrict the establishment of compartments that have repercussions beyond the originating department, and

- raise the level of classification-consciousness throughout the government.

The Study finds significant Agency noncompliance with the provisions of E.O. 11652. The principal areas are over- and unnecessary classification, excessive use of the exemption provision, and anomalous handling of Top Secret cables. Due to bureaucratic pressures and the force of precedent, classification errors made in the past tend to be perpetuated. Original classifiers, who are usually busy supervisors, often abdicate their classification responsibilities to subordinates. The "play-if-safe" mentality is a powerful contributing factor to overclassification. As remedies, the Study recommends:

- the establishment of a CIA Classification Board to replace the present CIA Information Review Committee,
- new guidance and stepped-up training in classification,
- the beginning of classification of documents by section or paragraph,
- the preparation of internal CIA guidelines for de novo classification of information taken from raw reports for use in finished intelligence,
- the handling of Top Secret cables in the same manner as other Top Secret collateral material,
- the abolition of pre-printed Secret forms,
- a thorough review of the number and level of authorized classifiers within the Agency,
- a new regulation on administrative privacy,
- research into means of controlling the reproduction of classified paper.

In assessing the effect of the classification system on day-to-day operations within CIA, the Study concludes that, except for Top Secret, the flow of information within the Agency, even when accompanied by overclassification, is only slightly impeded in reaching proper users.

- But the cumulative effects of overclassification are more insidious: Bad secrets devalue good ones, setting in motion a process of escalating protection for the "real" secrets which drains the classification criteria of their prescribed meaning.

- The regular classification categories have thus become the underpinning for a vast superstructure of supplementary protection. The latter includes not only the codeword compartments, but also the array of document control markings and the mini-compartments employed by the Operations Directorate to protect sources and methods.

The computer system of the Central Reference Service (CRS) recognizes some 1400 combinations of document control markings. The latter not only complicate retrieval of information, but sometimes preclude it altogether when, for reasons of sensitivity, documents are not indexed in the Agency's central reference system.

- The Study concludes that a DDO dissemination, stamped Secret and invested with some of the more restrictive handling controls, probably enjoys greater protection than the average Top Secret collateral or Top Secret codeword document. These access-limiting and distribution-control devices, and the special handling devices within the DDI, have a very tangible effect on the flow of information within the Agency.

- Although not taking a stand against these techniques, the Study points out that the lack of formal criteria for their use and their irregular application sometimes deprive analysts and operators of the information they need to do their job.

FOIA and the Privacy Act are having a significant impact on the Agency and on the functioning of the classification system within the Agency. The statutory and judicial aspects of these Acts place a premium on strict compliance with the classification and exemption provisions of E.O. 11652 and on quick discernment of overclassification in disputed cases. In the long run, they should have a corrective influence on classification abuses.

After examining the origins and judicial history of the sources-and-methods provision of the 1947 National Security Act, the Study concludes that, as it stands, the provision is an imperfect vehicle for protecting intelligence information from disclosure. Other statutory and constitutional barriers to disclosure are also examined and found wanting.

- The Study judges that the Atomic Energy Act of 1954 establishing the category of "Restricted Data" is perhaps the most successful security program in the government and may have value as a paradigm for statutory protection of foreign intelligence information.

The Study recommends, after reviewing legislative proposals for establishing a statutory classification system, as well as proposals for codifying the Espionage and related statutes and for strengthening the sources-and-methods

provision, that the Agency sponsor legislation amending the sources-and-methods provision, defining it, and establishing a new category of legally protected information, overlapping with, but independent of, the classification system.

- It recommends finally that the DCI, acting within the NFIB structure, create a committee of legal experts to study the revision of the Espionage Statutes.

DEVELOPMENT OF THE CLASSIFICATION SYSTEM

Information has been protected in one way or another from the very beginning of this country. The Constitutional Convention of 1787 conducted its proceedings in secret, and not until 1920 were the records of the Convention made public. The 1775 Articles of War, and legislation since 1776, have prohibited soldiers from corresponding with the enemy and civilians from spying in wartime.

During the Civil War, the government suspended habeas corpus, made numerous political arrests, and censored the press. After the Civil War, there was a gradual recognition of the importance of protecting military installations and the information concerning them from the prying eyes of foreign intelligence. Up to World War I, there was only one "classification"--Confidential--used to designate certain types of defense information requiring protection. But, unlike its modern namesake, the word "Confidential" had no prescribed meaning in terms of the contents of a document, but was rather a means of limiting the distribution to specified addressees or categories of addressees. Nor was it generally used to stamp documents.

Influenced by British and French example, the American Expeditionary Force in 1917 adopted multiple levels of classification--Secret, Confidential, For Official Circulation

Only--which were soon incorporated in War Department Regulations. But the use criteria for these document markings were based on a vague determination that a given piece of information was "more or less secret" and on a prescribed narrowing of the addressees according to the determined level of sensitivity. Though some see in this World War I experience the beginnings of the present classification system, its lineaments are much clearer in the 1936 revision of Army Regulations, No. 330-5, where, for the first time, the levels of classification were defined in terms of damage to national security, and the protection of the markings was extended to non-defense information affecting national security. The category, Restricted, however, which had now replaced Official Use Only, was really not a national security marking but rather a means of ensuring administrative privacy.

Although there are no close parallels to the present classification system in the pre-World War I period, there are nevertheless archetypes of several closely related security practices still in vogue today. Thus, General Orders, No. 3 of the War Department, 16 February 1912, prescribed these measures for safekeeping military records concerning seacoast defenses: They were to be "classed" as Confidential, kept under lock, given serial numbers, logged, subject to copy control, shown only to "trusted employees" according to the "exigencies of service." War Department

Regulations of 1913 ordered double wrapping of telegrams and other communications, with Confidential stamped on the inner envelope only. The Chief of Artillery complained bitterly in 1907 about the indiscriminate use of Confidential on Army issuances, citing in particular one that contained the formula for making whitewash. (This is perhaps the first documented instance of "unnecessary" classification.)

While the military were protecting their secrets by means of classification, the State Department, up to 1958, was still relying on the "housekeeping" statute of 1789 to protect diplomatic secrets. The first Executive order dealing with classification, President Roosevelt's E.O. 8381 of 1940, was essentially a wartime measure and had no lasting influence on classification. President Truman's E.O. 10290 authorized any government agency to classify "official information the safeguarding of which is necessary in the interest of national security and which is classified for such purposes by appropriate classifying authority." Because of the vagueness of the "national security" standard, Truman's order was immediately attacked as an infringement of the First Amendment.

It was superseded two years later by President Eisenhower's E.O. 10501, issued 5 November 1953, which lasted almost twenty years until replaced by the present system. It redefined Confidential, Secret, and Top Secret, reduced the number of

agencies authorized to classify, and set a twelve-year limit, subject to some exceptions, on maintenance of information in the Top Secret category. President Kennedy in 1961 (E.O. 10964) added provisions for automatic downgrading and declassification.[2] President Nixon ushered in the present system on 8 March 1972 with E.O. 11652 entitled, "Classification and Declassification of National Security Information and Material."

A National Security Council Directive implementing this Order was issued on 17 May 1972. The Order itself, which took effect on 1 June 1972, refined the criteria for the three levels of classification, replaced the "national defense" formulation of E.O. 10501 with that of "national security," a collective term for "national defense" and "foreign relations," established a general declassification schedule with four exemptions, and created an Interagency Classification Review Committee (ICRC) to assist the National Security Council (NSC) in monitoring the system.[3]

Criticism of the Classification System

It is hardly an exaggeration to say that the classification systems created by Executive order have been under almost continuous attack by Congressional and other bodies since their inception. The chief critic has been the House Subcommittee on Information, established in 1955, and joined

later in that role by the Senate Subcommittee on Intergovernmental Relations. The Freedom of Information and Privacy Acts were by-products of this close monitoring of government secrecy. A principal target of the House subcommittee in its early years was the functioning of the classification system within the Department of Defense. Reacting to Congressional pressure, the Pentagon established the Coolidge Committee to conduct an in-house investigation. This committee, and others since, directed attention to shortcomings that are still evident in classification practices today.

In its report, the Coolidge Committee concluded that the two major shortcomings of the system at that time were over-classification and deliberate unauthorized disclosure. The latter was a reference to the spate of disclosures prompted by interservice rivalry. The report found a tendency on the part of Pentagon officials to "play-it-safe" and overclassify; abuse of security in the classification of administrative matters; attempts to classify the unclassifiable; confusion stemming from classification procedures that were based on shifting foreign policy; and a failure to declassify material that was no longer secret.[4]

Reflecting the security concerns of the McCarthy era, the Congress in 1955 established a Commission on Government Security (known as the Wright Commission) that included

classification among the subjects it investigated. The section of the Commission's 807-page report, issued in 1957, dealing with classification, recommended "that the Confidential classification be abolished. The Commission is convinced that retention of this classification serves no useful purpose which could not be covered by the Top Secret or Secret classification."[5] It based this recommendation on a finding that overuse of Confidential was impeding the free exchange of scientific and technical information and thus hampering national security. (As will be seen in a later section, the abuse of Confidential then was similar to the abuse of the Secret label now.)

The Commission urged also the enactment of legislation making it a crime to release to an unauthorized person information classified Secret or Top Secret, knowing it to have been so classified, for any reason whatsoever. The bill was aimed at persons outside the government, such as newsmen, and aroused a storm of protest.[6] Noting that there were 1.5 million employees in the government authorized to classify documents, the Commission also recommended a major reduction in the number of classifiers.

Meanwhile, the House Subcommittee on Information (known as the Moss Committee after its first Chairman, Representative John E. Moss), having finished its investigation, delivered

its report in June 1958. The following excerpt is indicative of the tenor of the report:

> In a conflict between the right to know and the need to protect true military secrets from a potential enemy, there can be no valid argument against secrecy. The right to know has suffered, however, in the confusion over the demarcation between secrecy for true security reasons and secrecy for "policy" reasons. The proper imposition of secrecy in some situations is a matter of judgment. Although an official faces disciplinary action for the failure to classify information which should be secret, no instance has been found of an official being disciplined for classifying material which should have been made public. The tendency to "play it safe" and use the secrecy stamp, has, therefore, been virtually inevitable.[7]

The committee's recommendations, many subsequently embodied in the present E.O. 11652, called for a reduction in the number of classifying agencies and individual classifiers, an acceleration of the process of downgrading and declassifying, and establishment of an appeals procedure against misclassification.[8]

The final days of E.O. 10501 were characterized by spectacular leaks and acute administrative difficulties. In June 1971, a Top Secret study on Vietnam, the "Pentagon Papers," was published with impunity. This was undoubtedly the most flagrant and brazen violation of security in the history of the American classification system. That much of it was overclassified and that one would be hard put to prove that the disclosure caused "exceptionally grave damage to the nation" (to measure it against the then criterion for

Top Secret) is beside the point. In December 1971, there was a leak in connection with the India-Pakistan war; in early 1972, a National Security Council memorandum revealing policy conflicts over Vietnam war strategy appeared. All three instances exemplify unauthorized disclosure motivated by opposition to government policy. Their counterpart, and perhaps their inspiration, was the executive branch practice of selective disclosure and premeditated leaking to promote government policy.

On the administrative side, Congressman William S. Moorhead, the new Chairman of the Subcommittee on Government Operations and Government Information, referred to "mountains of classified documents" that had accumulated, contending that "the inevitable was finally recognized in early 1971 as massive overclassification and other abuses of the system created a classification crisis and the virtual breakdown of our system."[9]

Although one can doubt that the situation was as cataclysmic as this, it was sufficiently serious to prompt President Nixon to appoint, on 15 June 1971, an interagency committee charged with making a searching review of the classification system. The committee was headed by then Assistant Attorney General, William H. Rehnquist. After more than a year of study, the committee, early in 1972, presented a draft issued shortly thereafter as Executive Order 11652.

Since the issuance of E.O. 11652, Congressional criticism has made such points as the following:[10] (These points have figured prominently in the Congressional hearings on classification and, as we shall see further on, some of them are reflected in proposed legislation. The Freedom of Information and Privacy Acts, also discussed below, embody some of the thinking implicit in these criticisms.)

- "It confuses the legal meaning of the term 'national defense' and 'national security' and the terms 'foreign policy' and 'foreign relations' while failing to provide an adequate definition of these terms." (The reference is to the use of the term "national security" in E.O. 11652 in place of "national defense" used in E.O. 10501 and similar wording in Exemption (b)(1) of the Freedom of Information Act: "matters under Executive order required to be kept secret in the interest of national defense or foreign policy.")

- There are no specific penalties for over-classification and unnecessary classification.

- It permits defense and foreign policy errors to be concealed for at least three 4-year Presidential terms, and up to 30 years or longer under the exemptions.

- The ICRC is not accountable to Congress.

- Section 9 legitimizes and broadens authority for the use of special categories of "classification governing access and distribution of classified information beyond the three specified categories." (This refers to the authorization of supplementary protection such as codeword compartments and document control markings.)

- An independent regulatory body, with administrative, enforcement, and adjudicatory

powers, should be established in the executive branch to police all aspects of the classification system.

- A statutory classification system should replace the practice of Executive orders governing classification.

Congressional critics of the classification system have paid particular attention to the number of authorized classifiers. Seeing a causal connection between the expanding volume of classified information and the number of classifiers, they have demanded sharp reductions in the number of the latter. Thus, the executive branch was induced to reduce the number of classifiers from 1.5 million in 1957 to 55,000 in 1971, the year prior to the issuance of E.O. 11652. The 55,000 figure consisted of 2,849 Top Secret classifiers, 18,029 Secret, and 34,122 Confidential.[11] (The CIA figures for classifiers, given below, are the reverse of these, with the Confidential category being the smallest and the Secret the largest.)

But there is little evidence of a corresponding decline in the birth rate of classified paper.* Actually, no one knows the exact number of classified documents in the executive branch, not even the number of Top Secret ones. But the order of magnitude is ascertainable. Hearings of the

*We note, however, that the ICRC Progress Report for 1975 claims a 2 percent reduction in the number of classification actions in 1974 and 6 percent in 1975.

House Subcommittee on Information in 1971 and 1972 provide some bench marks: William G. Florence, a retired Air Force classification official, estimated that the Defense Department had at least 20 million classified documents and was of the opinion that 99 percent of them did not merit classification in terms of a strict interpretation of the Executive order. A State Department witness gave an estimate of 35 million classified documents for his department. And Dr. James B. Rhoads, the United States Archivist, said he was responsible for 470 million pages of classified material covering the period 1939-1954.[12] It would probably be safe to say that total classified holdings of the executive branch at this time have long since passed the billion mark.

There are grounds, therefore, for questioning the assumption that limiting the number of classifiers necessarily restrains the accumulation of classified paper. As indicated later in the CIA context, strong bureaucratic forces tend to undercut this assumption.

THE FUNCTIONING OF THE CLASSIFICATION SYSTEM WITHIN CIA

Our retrospective glance at the classification systems has shown the persistence of the following negative, seemingly ineradicable, characteristics: overclassification, unnecessary classification, vagueness of classification criteria, unauthorized disclosure, and the relentless accumulation of vast quantities of classified paper. Unfortunately, these traits are all relevant to the classification experience of CIA. In discussing classification within CIA,* the following questions are addressed:

- What is the incidence of abuses of classification, and the reasons therefor?
- How do the mandatory review provisions of E.O. 11652 affect the Agency?
- What is the impact of the Freedom of Information and Privacy Acts on the Agency and on the functioning of classification within the Agency?
- To what extent, if any, has the Agency failed to comply with the Executive order on classification?
- What is the effect of classification on the Agency?

The problem of unauthorized disclosure is considered from two perspectives:

- Faced with the problem of protecting foreign intelligence information and preventing unauthorized disclosure, what judicially enforceable sanctions are available to the Agency?

*The CIA regulation implementing E.O. 11652 is [redacted] revised 11 February 1975.

- What can be done within the Agency to improve the classification system, its management, and the protection of foreign intelligence information from unauthorized disclosure?

Misclassification

As of 31 December 1975, the CIA had 1,975 original classifiers, broken down as follows: 553 with Top Secret authority, 1,358 with Secret, and 64 with Confidential. The fact that the wielders of the Secret stamp are clearly in greatest demand suggests a positive correlation between the number of Secret classifiers (which includes also the Top Secret ones) and the overwhelming number of collateral documents bearing that classification. Up until about two years ago when the Director reacted against the wholesale abuse of the Secret classification, the use of the Confidential classification was relatively rare in the Agency. There were offices at that time where one could not find a Confidential stamp. It had become a reflex action to place Secret upon a piece of paper. If the officer forgot to do it, the secretary did so automatically. Given this automatism, which is far from being extinct, the total number of authorized classifiers tended to have a minimal effect on the total amount of classified paper produced. The hierarchical bias of the Agency suggests that the 1,975 classifiers mentioned above are by and large busy supervisory personnel who have little time to devote to the subtleties of

the classification system. They tend to accept the decisions of the subordinate non-classifiers. The number of de facto classifiers, therefore, far exceeds the number of authorized classifiers.

The problem confronting the conscientious classifier, once he has decided that a document should be classified, is to determine, according to the Order, whether the unauthorized disclosure of the information could reasonably be expected to cause: "exceptionally grave damage to the national security" (Top Secret), or "serious damage to the national security" (Secret), or "damage to the national security" (Confidential). National security is viewed as a hybrid of national defense and foreign relations. Examples are given in the Order for Top Secret and Secret, but none for Confidential. "Examples of 'exceptionally grave damage' include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communcations intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security." A strict application of these norms would substantially reduce the number of Top Secret documents, both collateral and compartmented. Persons interviewed have cited such egregious examples of overclassification as the following: NSA's Top

Secret city map of Moscow; a request for a computer terminal from one CIA component stamped Top Secret; the Top Secret NSCID 6 dealing with COMINT which, according to an Agency COMINT specialist, should at most be Secret.

For Secret level classification, the Order gives these examples of "serious damage to the national security": "disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security." One of the most prolific causes of abuse of the Secret classification is the widespread use in the Agency of pre-printed forms reading: "Secret When Filled In." This leads to such patent misclassification as Secret time and attendance cards, pay roll slips, etc. for overt employees. Should the Agency telephone book containing only the names of overt employees be classified Secret? Would its disclosure do "serious damage" to national security, or simply "damage," or no damage at all? Or should it be simply labeled "Internal Use Only?"

Fitness reports, investigatory reports, the whole field of administrative correspondence, is a fertile field for overclassification and often unnecessary classification. In this field, there is undoubtedly a great deal of confusion between

the legitimate needs of privacy and the classification criteria that relate exclusively to the protection of information whose disclosure would cause some degree of damage to national security. The Clandestine Service has a propensity for Secret that tends to blot out the other classifications. Some progress has been made, it is true, in downgrading most administrative matters to Confidential, but in the operational domain the Secret classification is so ingrained that the use of Confidential is still relatively rare. The mere presence of a cryptonym or pseudonym is often sufficient to dictate the use of the Secret stamp. Some analysts in both the DDI and the DDS&T have reported that it is generally the practice in their shops to publish at the highest level on the grounds that their high-level customers have all the clearances and that this gives greater status to the report. In one instance it was standard practice to include some codeword material so that the report could be printed the same day in a quick seventh-floor press setup, rather than sent to the Printing Shop, which would have entailed a delay of a day or so. This catalogue can be concluded by noting that the Confidential NSSM 229, establishing an ad hoc group to study classification procedures, is itself an example of unnecessary classification.

The most imprecise of the classifications is Confidential. The Order gives no explanation of what constitutes "damage" to national security, the criterion for Confidential. Still, it

requires little acumen to question the appropriateness of the Confidential classification on Credit Union statements of overt employees. Or the use of the Confidential stamp whenever an analyst expresses an opinion in writing. It is true that some opinions emanating from an official source could cause damage to our foreign relations, but it is highly unlikely that this is routinely the case. One senior DDI officer has expressed the view that most OCI non-codeword publications could almost be written at the unclassified level.

But, the reader may ask, what harm is there in overclassifying? The classifications all give protection, and that is what we are seeking, is it not? Unfortunately, classification abuses have side effects, both short-term and long-term, which cause significant difficulties for the CIA. Before describing these side effects, some other aspects of misclassification must be examined first.

Related Issues

Implicit in the description of the three levels of classification is the inherent vagueness of the classification criteria in the Executive order and the consequent play this offers to the subjectivity of the classifier. "The problem," according to Professor Stanley Futterman, "is that the classification system rests entirely on subjective decisions about contingent political effect."[13] In a section entitled

"Resolution of Doubts," the NSC implementation directive for E.O. 11652 recognizes the casuistical problems that may confront the conscientious classifier: "If the classifier has any substantial doubt as to which security classification category is appropriate, or as to whether the material should be classified at all, he should designate the less restrictive treatment." As early as 1961, former Defense Secretary Robert McNamara offered a similar admonition: "...I suggest that we follow this principle: when in doubt, underclassify."[14] There is unfortunately very little evidence that either of these precepts has ever had a significant following.

In addition to the problems posed by the criteria as such, the casuistry of classification must also contend with certain esoteric aspects of secrecy itself. These revolve largely around information that is unclassified in itself but for various reasons, rightly or wrongly, is treated as secret. A safe combination, not secret in itself, merits that status because of what it gives access to.[15] A Department of Defense affidavit given the court in connection with the "Pentagon Papers" case against the Washington Post stated: "It is sometimes necessary to classify a document in which no single piece or part is itself classified."[16] This is a valid point if the organization of the material, the mosaic effect superimposed on the unclassified pieces, meets the classification criteria. Often, however, the argument is specious. This is particularly

true of lists and compilations of unclassified items. E.O. 11652 contains this injunction: "Material containing references to classified materials, which references do not reveal classified information, shall not be classified." One may also be skeptical of the contention of one component of the Clandestine Service that the subjects of certain of its sensitive reports are not only Top Secret, but so sensitive that they cannot be included in the index of the Central Reference Service.

There is also secrecy by proximity or relationship, what has been referred to as the "layered secret."[17] A legitimate secret is surrounded by successive layers of secrecy. One must in these cases verify continually that the core secret remains a secret and that the protective layers are necessary and kept within reasonable limits. Some aspects of overhead reconnaissance illustrate well both the good and bad features of the layered secret.

There is the attempt to protect what really can't be protected: the self-revealing "secret." The launching of the Department of Defense Program 647 Early Warning and Surveillance Satellite is a typical example. "No declassification of information regarding the operation of that important and highly expensive vehicle has been permitted, even though news media and a Congressional committee have reported publicly how it functions. The system is so extensive in scope that it exposes itself."[18]

Finally, there is the "secret" which, through tacit agreement between two countries, is designed to avoid confrontation. The secret is based on political rather than security considerations. The Soviet Union is aware of our overhead reconnaissance program, just as it and the whole world is of our connection with the Glomar Explorer. In neither case, however, does the government officially acknowledge that connection. In the latter cases, unlike the situation that prevailed before the Soviets shot down the U-2 plane, the "secrets" are no longer bilateral and related to national security, but universally known "nonsecrets." The wisdom of the decision to avoid official acknowledgement is not in question, but the formalistic use of the classification system to continue to protect these "nonsecrets" is subversive of the system.

Although original classification for each level is in principle limited to classifiers designated in writing for that level by higher authority, there is no restriction on the proliferation of classified material through carry-over of classification from one document to another. To take an extreme case, but not an unusual one, a classified item representing perhaps one percent of an otherwise unclassified document will suffice to confer its classification on the whole document. Both the Order and the implementing directive are rigid on this point. One can easily see the potential for overclassification in this procedure. Typically, the

CIA analyst producing a piece of finished intelligence will use information from several sources and, in the process, often paraphrase or otherwise change the form of the original information, thus effecting in many cases a de facto sanitization of the original material. Yet he must carry over the original classification and give to the document the highest classification of the incorporated elements or go through the time-consuming process of negotiating a change of classification with the original classifiers. This problem is compounded by the Agency's failure to comply with those provisions of the Order and Directive requiring that, where practicable, documents be classified by paragraph. Thus a paragraph that deserves no classification or at most a low one would have to be taken over bearing the high overall classification of the document from which it was extracted. Many concerned with this problem have come to believe that a more rational approach would be de novo classification of finished intelligence products.

Reasons for Misclassification

The foregoing discussion has assumed a conscientious, rational classifier contending with the arcana of classification and the rigidities of the present system. Such a classifier is probably the exception. The persistent phenomena of overclassification and unnecessary classification can only be understood in terms of the classifier beset by

bureaucratic pressures and the powerful force of precedent. Decisions made in the past tend to be perpetuated indefinitely. How much easier it is to take over perfunctorily the classification of a reference or of similar material already published or in project files than to deliberate each time on the degree of damage to national security. There thus emerges what has been termed "inherited classification."[19] This mindless process probably accounts for a major portion of misclassified material.

There is also, on the part of some, an exaggerated conception of sources and methods which tends to see almost everything connected with the Agency as classified. The elitism referred to above in connection with publishing for a very select audience tends to counteract the pressure to publish at the lowest possible level.

Why is it, one may ask, that these abuses of classification are not corrected by the more perceptive in the Agency? The Order enjoins that if a holder of classified information believes "that there is unnecessary classification, that the assigned classification is improper, or that the document is subject to declassification under this order, he shall so inform the originator who shall thereupon re-examine the classification." But, in practice, this is never done. Instead, there is a kind of vicious circle described in the

illustrations above, with the supervisors too often relying on their subordinates, and the subordinates on tradition and precedent.

The basic reason, however, the reason that subsumes all these considerations, is that the present system is tilted in favor of overclassification. The calculus of risk for the classifier in over- or unnecessary classification is less than in underclassifying. "And since everyone believes that over-protection has less serious results than under-protection, overclassification is tolerated and shortfalls in judgment are excused."[20] There are, it is true, pro forma instances of persons in the Agency who have been notified that their actions were in violation of the terms of the Order and a few who have received an "administrative reprimand" for repeated abuse, but the overall effect has been slight.[21] Nor has the National Security Council, charged with monitoring the implementation of the Order, nor the Interagency Classification Review Committee (ICRC), created to assist the NSC in this task, been any more successful in rooting out misclassification. Playing-it-safe has thus become the rule of the game.

Anomalies in the Handling of Top Secret Material

There are approximately 129,500 collateral (non-codeword) Top Secret documents in CIA, and the Operations Directorate

accounts for more than 90,000 of them. These figures relate to documents other than cables. (For the latter there are no reliable estimates since they are not subject to mandatory logging and copy control.) In the neighborhood of 1100 Top Secret collateral documents are generated by the Agency each year. In addition, during 1975 CRS handled 444,870 codeword disseminations, of which perhaps 20 percent, in any case many times the number of Top Secret collateral cables, bore the Top Secret classification.

It is anomalous that the CIA Top Secret Control Officer has no responsibility whatsoever for Top Secret cables or codeword material. Once a Top Secret cable leaves the Cable Secretariat, it ceases to be the responsibility of the latter and is not subject to centralized record keeping, as are Top Secret collateral documents. Nor is there mandatory logging or copy control of Top Secret material within the codeword compartments. There is a computer program for keeping track of Top Secret collateral material, but neither Top Secret cables nor codeword material form part of the program. Unlike Top Secret collateral, where the recipient is supposed to acknowledge by his signature having seen a document, there is generally no record of those who see codeword material. If the often-made contention be accepted as true that Top Secret collateral is better protected than Top Secret compartmented information, then we have a further anomaly: a system designed to provide supplementary protection

per Section 9 of the Order providing less rather than more.

How much protection do Top Secret collateral procedures really provide? When followed to the letter, a considerable degree. But there are indications of deficiency on several fronts: First, it is not uncommon for the secretary of a unit to sign the control sheet of the document, which is then read anonymously by others in the unit. Copy control is often subverted by the Xerox machine. This was particularly true during the Congressional investigations when a considerable number of unnumbered copies of Top Secret documents were turned over to the committee investigators, before the practice was ended. Annual inventorying of Top Secret collateral documents has, in the past, been somewhat erratic. Even at present there are more than 16,000 Top Secret documents in the Agency which can't be located.

This discussion would be incomplete without passing reference to the pseudo-classification, "Top Secret Sensitive." Totally devoid of any authoritative basis, its only rationale is convenience. Circumventing the codeword compartments, it brings together in one place all-source information in a collateral format. The uses that have come to the attention of this Study are the following: The daily cable summary for the DCI (seen by nine persons in the Agency); the Intelligence Checklest (until recently sent to five committees of Congress); and use as a classification on codeword material released to

foreign chiefs of state (when authorized by the DCI on a highly selective basis). Its proponents argue that it is the only feasible means, in these and similar situations, of transcending, in timely fashion, the complexity of cumulative codewords and dissemination controls.[22]

Exemption, Downgrading, and Declassification

In a totalitarian society, downgrading and declassification of information have little or no meaning. It is only when the ideal of an informed citizenry is accepted and acted upon that these procedures have any chance of catching the attention of management. The Freedom of Information Act was passed in 1966, but was relatively ineffective until teeth were put into it in 1974. Since February 1975, the effective date of the amended Act, the whole subject of classification, particularly declassification, has become an important concern of U.S. Government management. The new DCI emphasized this point on 13 May 1976 in his Guiding Principles for the Intelligence Community: "We have an obligation to provide as much information as possible on an unclassified basis, but without derogation of the necessity to protect sensitive sources and methods and to protect information which truly requires sensitive treatment." The Privacy Act (PA), which became effective on 27 September 1975, has also had the effect of refining the Agency's perception of classification.

It is against this background that the conscientious classifier described above must approach another duty prescribed by E.O. 11652. In addition to determining the degree of damage to national security that disclosure would entail, he must gauge how long the information will require this level of protection. His options are these: to subscribe to the timetable of the General Declassification Schedule (GDS), to specify a date or an event earlier than the GDS for declassification, or, judging that the information requires greater protection than that provided by the GDS, to exempt it from the operation of the GDS. This he may do if the information falls into one of four exemption categories specified in Section 5(B) of the Order and providing he specifies the category and, unless impossible, a date for automatic declassification. Exemption 5B(1) protects confidential information provided by foreign governments or international organizations; 5B(2) deals with information or material "specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources and methods"; exemption 5B(3), the broadest of the categories, protects information "disclosing a plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security"; exemption 5B(4) exempts information "the disclosure of which would place a person in immediate jeopardy." (Hereafter for convenience we shall refer to the exemptions as E1, E2, E3, and

E4.) The Order requires that "the use of the exemption authority shall be kept to the absolute minimum consistent with national security requirements..."

Despite the foregoing, downgrading and declassification, except as triggered by external requests under FOIA, PA, or under E.O. 11652 for classification review, are relatively rare within the Agency. This is because almost the entire classified product of CIA is routinely exempted, usually under E1 and/or E2.[23] The propriety of this wholesale use of the exemption clause is difficult to assess directly, but it is at the very least highly suspect. When few in the Agency can recall ever having seen a classified piece of CIA paper without E.(1), or E2 IMPDET on it, there are grounds for doubting that the use of the exemption authority is being kept to an absolute minimum. The truth is that the automatism that we found in the case of classification is even stronger and more prevalent in this domain. Although the Order stipulates that only a Top Secret classifier may exempt, it is commonplace throughout the Agency for secretaries to affix E2 IMPDET to just about every classified piece of paper they type. Even granting that most of the paper generated by the Agency deserves to be exempted, this still leaves a large amount that doesn't, that simply falls victim to another play-it-safe routine. There is no gainsaying the short-run advantages of this approach, though

contrary to the Order, in terms of convenience, economy of time, and fool-proof protection of information.

By invoking the exemption authority the classifier bypasses the automatic downgrading timetable of the GDS (Top Secret to Secret two full calendar years after origination, Secret to Confidential two, Confidential to declassified six) but, in the long run, the exempted material still comes up against mandatory review for declassification. This may occur at any time ten years after the date of the document's origination, upon request of a member of the public or another department. If the information no longer qualifies for exemption, it must be declassified. All classified information or material 30 or more years old must be declassified also unless the head of the originating department personally determines in writing that the information requires continued protection for a specified period. In both instances, the Directive provides that, if the final departmental decision on declassification is negative, a member of the public may appeal the decision to the ICRC, and, in that case, "the burden of proof," the Directive adds, "is on the originating Department to show that continued classification is warranted within the terms of the Order."

The wholesale exemption of information, the failure to conduct systematic reviews before retiring files to the Records Center, and the failure to label the unclassified portions of

documents--these practices have merely served to postpone decisions that must eventually be made on destruction, historical preservation, and declassification. With thirty-year review these decisions come home to roost, but magnified in number and complexity. For several years now a task force has been at work culling OSS documents that have passed their thirtieth year, and next year the first CIA documents, dating from 1947, must be reviewed. In the time frame--1947 through 1966--there are 13,579 cubic feet of records in the Agency Archives. Since these records are by and large segregated chronologically, the problem is not so much finding what has to be reviewed, as perusing thirty years later a vast accumulation of often unfamiliar documents and making decisions that could more easily have been made in the past. Without belaboring the point, it is clear that the task of the reviewer of old Agency files would have been considerably less complicated and less time-consuming if the files had been thinned out periodically by downgrading and declassification, if worthless documents had been destroyed, and if the remaining documents of historical interest had been sectionally classified.

Impact of Freedom of Information and Privacy Acts

The following figures for 1975 give some idea of the scope of the Agency's FOIA/PA program (the figures also

include requests for information under E.O. 11652): 5,859 requests for information were processed; 100 persons worked full time processing them; the more tangible costs totalled $1,392,000.[24] Since these are not full-year figures for either FOIA or PA, the figures for 1976 will probably be significantly higher. (The amended FOIA took effect in February 1975 and the PA in September 1975. From February 1975 until September 1975 privacy-type requests were processed under FOIA.)

Under the Privacy Act any American citizen or resident alien may levy a request on CIA for information concerning himself and, unless its disclosure would compromise sources and methods or cause damage to national security, it must be granted. On the other hand, anyone anywhere may request information under the provisions of FOIA and, unless the information falls in one of nine exempt categories, it must be released. Six of these categories are particularly relevant to CIA. Exemption (b)(1)--information properly classified pursuant to an Executive order--in effect gives statutory recognition to E.O. 11652.; (b)(3) exempts information specifically exempted from disclosure by statute. The other four, however, go considerably beyond the Order. Thus, the following categories of information, whether classified or not, may be withheld: (b)(2)--personnel rules and guidance;(b)(5)--records of deliberations; (b)(6)--personnel

and medical files; (b)(7)--investigatory files of five specified types. These exemptions are of interest not only in their own right, but also because they provide protection for information that, as we have seen before, has often been erroneously classified under E.O. 11652. Seven of the exemptions (all except (b)(1) and (b)(3)) are discretionary in nature, but the Attorney General has ruled that information should be withheld only when it is "necessary or desirable in the national interest."

Under the terms of both laws, if information is withheld and the requestor seeks legal redress, the district court may examine the propriety of both the classification of the information withheld and of the exemption invoked. Section 552 (a)(4)(B) of the FOIA declares that the district court has jurisdiction "to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection(b) of this section, and the burden is on the agency to sustain its action."

The following table is a breakdown of the action taken by CIA on the 5,859 requests for information processed during

25
1975. (The vast majority of these requests concerned, in order, the Operations Directorate, the Office of Security, and the Office of Personnel.)

	FOIA	PA	EO*
Total Final Responses during CY 1975:	5,479	196	184
a. Granted in full	300	4	63
b. Granted in part	428	3	88
c. Denied in full	174	0	28
d. No record available, etc.	4,577	189	68

*This includes requests from a member of the public or another government department under the mandatory review provisions of Section 5(C) of the Order.

The 886 requests granted in whole or in part involved declassification of documents that had been classified up through Top Secret and almost without exception exempt from downgrading.

As of 30 September 1976, litigation stemming from requests for information had produced these results at the district court level: ten cases won (appeals pending on three of them), none lost. Two dealt with the Agency's refusal to release information concerning its budget; one with the Glomar Explorer; one with the "Bay of Pigs"; one with Congressional documents held by the CIA; and five with requests for information contained in CIA personnel files. Commenting on these results

and our experience to date, an officer who follows these programs closely remarked: "We've been forthcoming, but haven't given any secrets away."

The statutory and judicial aspects of FOIA and the Privacy Act place a premium on strict compliance with the classification and exemption provisions of E.O. 11652 and on discernment of overclassification in disputed cases. The leavening effect of FOIA/PA should eventually have a remedial influence on the abuses of classification discussed earlier. But for the Intelligence Community as a whole, they have created a new environment dominated by the interaction of three powerful forces: Privacy, Publicity, Secrecy.[26] Any reform of classification must reckon with these conflicting forces and attempt to establish a dynamic equilibrium among them.

Scope of Noncompliance with E.O. 11652

This is a convenient point at which to sum up the extent of Agency noncompliance with the Order and its implementing Directive and, at the same time, to consider the extent to which compliance with the Order is feasible.[26a] Unless otherwise indicated, the references below are to sections of the Order.

- Section 1: The failure to interpret strictly the definitions of Top Secret, Secret, and Confidential is the root cause of over- and unnecessary classification in the Agency. It does not appear that Top Secret, especially in the codeword compartments, has been used with "the utmost restraint."

- Section 3: As we have seen, there is practically no downgrading or declassifying until a member of the public makes a request for information, or until the obligatory review of thirty-year-old documents occurs.

- Section 4: This section lays down rules designed to prevent abuses of classification. Contrary to this section, a person is rarely held "accountable for the propriety of the classification attributed to him." Although the failure to enforce this section has probably contributed to the spread of over- and unnecessary classification, it has not drawn in its wake, as far as we can judge, those other abuses proscribed by this section: classifying information "in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative..."

  We have seen that the Agency does not show "to the extent practicable," which "portions" of documents are classified and which are not classified, as required by Section 4. The Directive specifies: "Whenever a classified document contains either more than one security category or unclassified information, each section, part or paragraph should be marked to the extent practicable to show its classification category or that it is unclassified." Although onerous, this requirement is hardly infeasible. Other departments, especially the Department of Defense, have substantially complied with it.

- Section 5: There is noncompliance on two counts: wholesale exemption of information and failure to declassify promptly exempted material no longer requiring protection.

- Section 6: Subsection (E): There is accountability for Top Secret collateral material, but not uniformly for Top Secret codeword material;

there is accountability generally in transmitting material outside the Agency, but not generally for Secret and Confidential within components. Subsection (F): There is no systematic review of classified material "no longer needed in current working files or for reference or record purposes" for destruction.[27] The counterpart of such a review is the identification of material that should be preserved and, where appropriate, marked for eventual declassification.

- Section 7(B)(3): Based on what we have seen above, the training and orientation programs for employees concerned with classified information appear inadequate; periodic reorientation programs during employment are generally nonexistent. (Formal Agency instruction on classification consists of: 45-60 minutes given to new employees by the Office of Security; about 20 minutes of a one-hour lecture also covering the FOIA and the Privacy Act, in the Office of Training's Operation Records I course.)

- Section VII of Directive: This section requires each department to undertake the establishment of a "Data Index System" for Top Secret, Secret, and Confidential material of sufficient historical or other value for preservation (the categories to be approved by the ICRC). The ICRC has accepted the AEGIS system of the Central Reference Service as compliance with this provision. AEGIS, however, contains only disseminated intelligence; the whole operational product of the Agency is excluded and, although much of the latter may not be of historical interest, this is certainly not true of material dealing with covert action, and many other types of operations.

There is evidence of considerable violation of Section VI G.(4) of the Directive which prohibits the reproduction of Top Secret information without the consent of the originating office.

- Section 13 (Administrative and Judicial Action): The pro forma enforcement of the penalties

prescribed by this section--notification and administrative reprimand--has been noted above.

Effect of Classification on the Agency

In terms of the classification Directive and Order, there are clearly shortcomings in the Agency's compliance. But, in terms of the collection and production of intelligence, what impact do our classification practices have? Do they significantly undercut the effective performance of our mission?

One observer of the classification system has written that there "is no threat to the Republic in the overclassification of trivia."[28] Does this dispose of the question? We have seen that indirectly, through statutory requests for information from members of the public, the effect on the Agency's classification practices has been considerable; and we have seen that henceforth review of Agency documents on their thirtieth anniversary will be immensely complicated. But what has been the effect on day-to-day operations? In an organization where everyone is Top Secret-cleared, simple classification, with the exception of Top Secret, restricts only slightly the flow of paper. In terms of access and storage, there is not much difference in the handling of Secret and Confidential documents. And the relative paucity of Top Secret collateral documents limits their quotidian impact. In this restricted context overclassification is probably not a "threat to the Republic."

There is, however, another context in which the effects, although subtle and elusive, are cumulatively more serious. In the long run overclassification saps the defenses of classification. Bad secrets depreciate good secrets. Thus, many within the Agency have come to believe that Secret alone has lost much of its meaning and some, out of zeal for security, buttress an item requiring only the protection of Secret with supplementary controls and markings or even find a way of insinuating it into one of the codeword compartments. This escalating protection accorded the "real" secrets, tends to drain the classification criteria of their prescribed meaning.

Simple classification has become the scaffolding for labyrinthine systems of supplementary protection. Paradoxically, the cause is not just overclassification, but also the permissive language of Section 9 of E.O. 11652 which, as we saw above, sanctions additional protection. In this context we think immediately of the codeword compartments, but there are other techniques, such as document control markings and the mini-compartments erected by the Operations Directorate to protect intelligence sources and methods, which are highly effective and, sometimes, more so than the former.[29]

The automatic data processing system of the Central Reference Service (CRS) recognizes some 1400 permutations of document control markings used in the Intelligence Community or by our allies.[30] This, despite the fact that

DCID 1/7, dated 5 October 1975, prescribes only five restrictive markings: ORCON, NFIB Departments Only, NOCONTRACT, PROPIN, and NOFORN. Of these, ORCON-"DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR"- is the most restrictive and the most controversial. It impinges not only on Agency customers who complain vociferously about it, but also, to a lesser degree, on CIA producers of intelligence. The markings in their totality have complicated enormously the job of CRS. A CIA Inspector General team concluded in a 1973 study that "the various elements of the Agency, in observing or instituting the handling restrictions affixed on intelligence documents, have compromised the retrievability of a significant amount of paper by excluding it from the Agency's central reference system. Such withholding has tended to assume a permanent character, without reference to either the changing sensitivity of the particular operation or the paper produced by it, or CRS's ability to ensure the application of the most stringent controls."[31]

Considerably more constricting are the DDO procedures for protecting sensitive information. These include: "RYBAT" for "highly sensitive operational correspondence," the "Prescribed and Limited Distribution" (P and L) for "exceptionally sensitive material," and "Restricted Handling" (RH), not covered by regulation but set forth in a book dispatch

for field stations, for the most sensitive material. The distinctive feature of the latter is that incoming traffic is not processed by the Cable Secretariat, but held by the Signal Center for pickup by designated persons.[32] Only a small number of persons, sometimes not more than 20 in the Agency whose names are entered on a bigot list, have access to RH traffic on a sensitive operation. The objective is to protect not only the identity of the source, but the very existence of the operation. (There has been considerable erosion in the effectiveness of the RYBAT procedure and some would add in that of P and L also.) Up to this point RYBAT, P and L, and RH concern primarily the DDO. But the intelligence information generated by the operations these procedures protect must be disseminated. This, in turn, gives rise to an array of access-limiting techniques that include multiple source descriptions, the "Particularly Sensitive Report" that is handcarried to addressees and receipted for, quasi-compartments with codewords for authorized recipients. "Exclusive For" reports can be as restrictive or more restrictive than P and L or RH-generated disseminations. The IG study mentioned above estimated that between 1,500 and 3,000 reports a year emanating from P and L and RH cases fail to reach the CRS because of sensitivity. This poses a serious retrieval problem, since this information is usually not indexed in CRS either.

Summing up, we come to the ironical conclusion that a DDO dissemination stamped Secret and surrounded by some of the more restrictive devices described above probably enjoys greater protection than the average Top Secret collateral or Top Secret compartmented document. In contrast with simple classification, these access-limiting and distribution-control devices have a very palpable effect on the flow of information within the Agency and on the production of intelligence. They are outgrowths, at least in part, of the lack of flexibility of the classification system and of the failure to use it correctly. These DDO devices and the special handling ones within the DDI and DDS&T restrict information to small numbers of officers, to certain classes of employees, even to certain elements within Divisions or Offices. This is not to say that they should not be used, but merely to emphasize that their inevitable spotty application and the absence of formal criteria for their use can and has led to situations in which analysts and operators lack the information needed to do their jobs.

THE PROBLEM OF DISCLOSURE

The Protection of Sources and Methods

The classification system applies to the executive branch as a whole, but the protection of "sources and methods" applies to CIA in a very special, almost unique way.[33] It overlaps with classification, but has an independent life; it is another means of protecting foreign intelligence information. Its statutory basis is Section 102(d)(3) of the National Security Act of 1947: "And provided further, that the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure; ..." Referring back to this latter provision, Section 6 of the CIA Act of 1949 exempts the Agency from the provisions of any other law which requires "the publication or disclosure of the organization, functions, names, official titles, salaries, or numbers of personnel employed by the Agency..." Note that it is the Director personally who is charged with the responsibility of protecting sources and methods and that there is no explicit grant of powers to be exercised in carrying out this responsibility. Nor is there a definition of the scope of "sources and methods." E.O. 11652 refers twice to "sources and methods": E2 excludes information "disclosing intelligence sources and methods" and Section 9

authorizes supplementary protection for intelligence sources and methods. The criteria for Top Secret and Secret mention respectively "sensitive intelligence operations" and "intelligence operations."

The origin of the "sources and methods" concept is somewhat nebulous. The earliest known references occur in military planning papers dealing with the establishment of a "central intelligence service." General William J. Donovan had submitted to the President in November 1944 recommendations for a post-war intelligence service and the President had instructed the Joint Chiefs of Staff to study them and to prepare a draft Executive order for his signature. In a memorandum, dated 18 January 1945, the Joint Strategic Survey Committee, commenting on a proposed draft recommended: "With a view to emphasizing the importance of protecting certain methods and sources of obtaining information the following should be added to paragraph 6 of the draft directive: 'In the interpretation of this paragraph, the National Intelligence Authority and the Central Intelligence Agency will be responsible for fully protecting intelligence sources and methods which, due to their nature, have a direct and highly important bearing on military operations.'"[34]

This wording was incorporated into the draft Executive order that the Joint Chiefs of Staff sent to the President

circa 18 September 1945. The pertinent portion of paragraph 7 of the draft reads: "As approved by the National Intelligence Authority, the operations of the departmental intelligence agencies shall be open to inspection by the Central Intelligence Agency in connection with its planning function. In the interpretation of this paragraph, the National Intelligence Authority and the Central Intelligence Agency will be responsible for fully protecting intelligence sources and methods which, due to their nature, have a direct and highly important bearing on military operations."[35] There is circumstantial evidence that this sources-and-methods formulation may have originated, at least indirectly, with the Navy, in particular with the Director of Naval Communications who expressed concern that the availability of military communications intelligence to the Central Intelligence Agency would be detrimental to military operations and therefore recommended inclusion in the draft directive of language permitting each department or agency to withhold such information if it felt that disclosure "will be inimical to the functions of such department or agency."[36] The sources-and-methods obligation was apparently the result of a compromise with those in the military demanding discretionary authority to withhold sensitive information from CIA. In any event, it is fairly clear that the wording was designed to ensure that CIA adequately protected military secrets.

"Sources and methods" were not mentioned in the CIA sections of the draft bill sent to Congress by President Truman in 1947. The White House felt that the CIA section should be kept as short as possible to avoid controversy and not jeopardize the main thrust of the bill which involved the unification of the armed services. Congress felt otherwise. The Central Intelligence Group accordingly submitted to Congress its recommendations (originally sent to the White House) containing the sources-and-methods language. As incorporated in the 1947 Act, the latter is in the form of a proviso, one of three provisos restricting the powers of CIA. The other two provisos respectively deny to the Agency police powers and, by authorizing departmental intelligence, a monopoly in the intelligence field. Although the explicit reference to military secrets found in the old NSSC version is dropped, the contextual implication of the obligation to protect sources and methods is almost that of a condition of access to the intelligence of other departments.[37]

However this may be, CIA legal thinking on the sources-and-methods obligation has seen in it a significant grant of implicit authority to the Director that goes beyond the mere protection of classified information. "The Congress use of the term 'sources and methods,'" writes the Assistant General Counsel, "indicates its recognition of the existence

of a special kind of data encompassing a great deal more than what is usually termed 'classified intelligence information.'"[38] And the CIA General Counsel in a letter to Senator Muskie, dated 13 August 1974, in connection with the Senate hearings on classification, declared: "...it is conceivable that certain intelligence sources and methods information would require protection under 403(d)(3) of Title 50 [United States Code designation of Section 102(d)(3)] even though it would not also warrant classification under the Executive order. Information protected under that subsection, whether or not classified, is not subject to the mandatory disclosure provisions of the Freedom of Information Act since that Act does not apply to matters that are specifically exempt from disclosure by statute."[39]

From these citations two thoughts emerge: that sources-and-methods information is not synonymous with classified intelligence information, and that it may even embrace information not classifiable in terms of the Executive order. It follows that sources-and-methods information has a specific character distinguishable from substantive intelligence information. One might define it as embracing:

a) information or material revealing or tending to reveal the identity and association with CIA of any person, group, organization, or governmental entity, whether witting or unwitting, that provides foreign intelligence information or intelligence-related services, as well as the identificiation and connection with CIA of any intelligence-producing device; and

> b) information or material revealing or tending to reveal the means, techniques, and procedures by which foreign intelligence is collected, processed, and analyzed, including those used to support and protect foreign intelligence activities, to the extent that these means, techniques, and procedures are subject to countermeasures, or revelatory of intelligence intentions and capabilities. It must be broad enough to include all forms of clandestine activity, as well as scientific and technical intelligence. And, of course, it must include sources-and-methods information furnished by foreign governments. Unlike much other sensitive information, it is difficult to prescribe in advance the life span of sources-and-methods information.[40]

The question naturally occurs, How have the sources-and-methods provisions fared in the courts? In the United States v. Jarvinen, a 1952 case, the United States District Court for the Western District, State of Washington, rejected the argument that two CIA employees, acting on instructions from the DCI under Section 102(d)(3), could refuse to testify in court concerning an informant of the CIA office in Seattle. They were sentenced to two weeks in jail, but later received a Presidential pardon. Because of the defective fact situation and the danger of creating an unfavorable precedent, the Agency decided not to appeal the decision of the district court.[41]

On the other hand, in Heine v. Raus, an action filed in 1964, there was a clear vindication of the Director's role in the protection of sources and methods. Confirming the decision

of the Maryland District Court, the Fourth Circuit Court of Appeals said, "action here to protect the integrity of sources of foreign intelligence was explicitly directed by Congress."[42]

Sources and methods figured also in the Marchetti case. Although the Supreme Court had refused the government an injunction in the "Pentagon Papers" case, the U.S. District Court for the Eastern District of Virginia in Alexandria issued an injunction on 18 April 1972 enjoining Victor Marchetti from public disclosure of any intelligence information, particularly that relating to intelligence sources and methods, and requiring him to submit his manuscript to the CIA for review before releasing it "to any person or corporation." The Fourth Circuit Court of Appeals restricted the injunction to "classified information" acquired by Marchetti during his employment by CIA.

In its final position on the Marchetti manuscript the Agency insisted on 168 deletions. The district court upheld only 26 of them, but, on appeal, the Fourth Circuit Court sustained the remaining 142 deletions and remanded the case to the district court "for such further proceedings as might be necessary." In his opinion of 7 February 1975 the chief judge of the Fourth Circuit Court, Judge Haynsworth, took note of the DCI's statutory responsibility to protect sources and methods, but based his decision on the classified nature of the information.

What was particularly noteworthy about the Marchetti case, however, was the willingness of the courts, under certain narrowly defined circumstances, to accept "prior restraint"--in this instance, because of the contractual nature of the secrecy agreement signed by Marchetti as a CIA employee.[43]

Since December 1975 there have been at least seven cases in which U.S. district courts have recognized the sources-and-methods provisions of the 1947 and 1949 Acts as a statutory basis, under exemption (b)(3) of the FOIA, for withholding information. Moreover, in most cases the courts have accepted testimony and affidavits rather than insisting on in camera examination of documents. Reaffirming the legal force of the sources-and-methods provisions, Judge William P. Gray of the U.S. District Court for the Central District of California declared in Stanley D. Backrack v. CIA, William Colby, a case decided on 13 May 1976: "While there is a strong public interest in the public disclosure of the functions of government agencies, there is also a strong public interest in the effective functioning of an intelligence service, which could be greatly impaired by irresponsible disclosure." Through the decisions of these district courts a series of precedents is emerging which have already greatly enhanced the legal stature of sources and methods as an independent means of protecting intelligence information--at least in the context of FOIA requests for information.[44]

The Agency's experience with the Marchetti case revealed certain weaknesses from a judicial review aspect in generalized appeals to Section 102(d)(3) as a means of preventing the disclosure of sources-and-methods information. To give greater legal solidity to future use of this Section, the Office of the General Counsel has drawn up a catalogue of sources and methods, hopefully broad enough and specific enough to prove convincingly in case of litigation that a disputed piece of information falls clearly in a category previously designated by the Director pursuant to his statutory authority.[45] Complementary to this is the draft DCID (1/19) entitled "Non-disclosure Agreements for Intelligence Sources or Methods Information." Paragraph 1 sets forth the policy: "All members of the Executive Branch and its contractors given access to information containing sources or methods of intelligence shall, as a condition of obtaining access, sign an agreement that they will not disclose that information to persons not authorized to receive it." The agreement is to make specific reference to Section 102(d)(3), and each protected document is to bear the marking: "Warning Notice: Sensitive Intelligence Sources and Methods Involved." When finally implemented, these two steps should go a long way toward filling loopholes that judicial challenges might otherwise have found. The shortcoming of both these steps,

however, is the absence of a definition of sources and methods. A catalogue excludes what it fails to include. Undefined, sources-and-methods information runs the risk of becoming as jargonized and abused a concept as that of "national security."

Statutory and Constitutional Barriers to Disclosure

> "American culture is a populistic culture. As such, it seeks publicity as a good in itself. Extremely suspicious of anything which smacks of holding back, it appreciates publicity, not merely as a curb on the arrogance of rulers, but as a condition in which the members of society are brought into a maximum of contact with each other. Favoring the exposure of practically every aspect of life, it is uneasy in the presence of those who appear to be withholding something."[46]

It is against this ethos that the torrent of unauthorized disclosures in the seventies must be viewed. These included the "Pentagon Papers" in 1971; the Marchetti and Marks expose in 1974; Agee's damaging book in 1975; and the Village Voice publication of the Secret report of the House Select Committee on Intelligence in 1976.

Besides the American penchant for publicity, disclosure at any particular time may be triggered by such factors as a disgruntled or disaffected member of the executive branch, sharp cleavages in the body politic, a confrontation between the Congress and the President, and secrets that have lost their credibility.[47] The "Pentagon Papers," which has been referred to perversely as "citizen disclosure," belongs to

the species designed to change government policy. As such, it has a number of precedents in our early history, although certainly not in scale or impact. In 1795 Senator Mason of Virginia, feeling that the people had a right to know the terms of a treaty that Washington had laid before the Senate in secret session, sent a copy to the Philadelphia Aurora; Senator Tappan of Ohio did the same thing in 1844 with a treaty calling for the annexation of Texas which President Tyler had presented to the Senate in secret session, sending the text to the New York Evening Post; and in 1848 the New York Herald Tribune published the Treaty of Guadaloupe Hidalgo ending the Mexican war, while the Senate was debating it in executive session.[48] The other three cases of recent disclosure illustrate the tension between publicity and secrecy at its tautest point, that is, as it relates to covert intelligence activities. In three of the four cases an essential ingredient was a disgruntled or disaffected employee or former employee of the executive branch.

It is striking that the compromises of classified information in the seventies have been overwhelmingly due to public disclosure rather than espionage. The legal defenses of secrecy, like the Maginot Line, have been so singlemindedly directed against espionage that they have been repeatedly outflanked by public disclosure. The First Amendment to the Constitution, in severely restricting the use of "prior restraint" against

the press, has also been, it is true, conducive to disclosure. In view of this situation, how much protection then do statutory and other judicially enforceable principles provide for foreign intelligence information?

Before there was a classification system or espionage laws, the executive branch protected secrets by virtue of the principle of "executive privilege." The authority for issuing Executive orders on classification derived from the exercise of this privilege.[49] E.O. 11652 refers only indirectly to the Espionage Statutes. The doctrine of executive privilege is an unwritten, implicit power that is usually derived from Article 1, Section 2 of the Constitution--the separation-of-powers provision--and, as it relates to national security, from the powers of the President as Commander in Chief and as the principal representative of the State in the conduct of foreign affairs. In the New York Times Company v. the United States, in 1971, even while refusing to support the government's position on the "Pentagon Papers," Justice Potter Stewart gave a ringing affirmation of executive privilege: "It is clear to me that it is the constitutional duty of the executive--as a matter of sovereign prerogative and not as a matter of law as the courts know law--through the promulgation and enforcement of executive regulations, to protect the confidentiality necessary to carry out its responsibilities in the fields of international relations and national defense."[50]

But the extravagant claims of executive privilege in connection with the Watergate experience and their rejection by the Congress and the courts have made incontrovertibly clear that the executive has no absolute power to withhold information for national security, or any other reasons, being subject in the exercise of executive privilege to legislative and judicial checks and balances. Executive privilege still remains a valid doctrine, but the courts are more likely to support the Executive in withholding valid state secrets than in preventing their publication once they have escaped from executive control.[51] This is certainly borne out by recent disclosure history.

One statutory barrier to disclosure--the sources-and-methods provisions of the 1947 and 1949 Acts--has been discussed in the preceding section. Exemption (b)(1) of the Freedom of Information Act gives statutory sanction to the protection of information properly classified in accordance with an Executive order.

A particularly operative statute is the Atomic Energy Act of 1954, which offers this definition of Restricted Data: "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data

declassified or removed from the Restricted Data category pursuant to Section 142." As perhaps the most effective security program in the government, Restricted Data merits our attention. A unique feature of Restricted Data that marks it off from national security information classified under E.O. 11652 is that by law any information falling within the definition above, no matter where it originates, is automatically classified, or, to use the expression of the Energy Research and Development Administration (ERDA) Handbook, is "born classified."[52] The open-ended nature of the definition is brought within reasonable bounds by Section 142 of the Atomic Energy Act which obliges the Commissioners collectively to declassify all Restricted Data that can be published without undue risk to the common defense and security.

Sections 142(c) and 142(d) require the Department of Defense and the AEC to determine jointly what Restricted Data relates primarily to the military utilization of atomic weapons; this information can then be "transclassified" and protected as national security information. This decompartmented atomic information then is known as "Formerly Restricted Data," and its passage to foreign countries, except by special agreement, is precluded. Section 142(e) permits the transclassification of atomic energy information pertaining to

other countries if the Commission and the Director of Central Intelligence jointly determine that the information is necessary for the intelligence process and can be adequately protected as national security information. This flexibility, coupled with ERDA's strict compliance with the declassification provisions of the Act, has contributed greatly to its success as a security program.

53

Next to Restricted Data, cryptographic information has probably been the category of classified information most successfully protected by statute. It is protected under the Espionage Statutes, which are codified in Sections 792-799 of Title 18 of the United States Code. Section 798 deals with cryptographic information. It criminalizes the publication or transmission to an unauthorized person of 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 ...(4) obtained by the processes of communications intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes..." It goes on to define "communications intelligence" as "all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." Section 798 specifically bans

publication of cryptologic information in unequivocal terms and omits the "intent" criteria of culpability which weaken the other sections. As it relates to the "procedures and methods" of communications intelligence, this statute overlaps to some extent with the sources-and-methods provision of the 1947 Act.

Section 793 of the Espionage Statutes penalizes a series of specified actions undertaken "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." The underlining, which we have added, is the guilt criterion common to this section and Section 794. Subsection (a) of Section 794 punishes with death or imprisonment anyone who delivers, or attempts to deliver, to a foreign person or government, information relating to the national defense with the intent formulation underlined above. Subsection (b) imposes the same penalties on anyone who, in time of war, "with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates..." information on troop movements, defense dispositions, etc. This is the only place in the Espionage Statutes where the "publishing" of defense information is specifically mentioned. It is limited in its application to time of war and to communications intended for the enemy. "If this intent requirement

is read to mean conscious purpose--a construction suggested by the absence of the "reason to believe" standard used in the culpability formulation of 794(a)--then prosecution of normal publication under Section 794(b) is a virtual impossibility."[54]

Returning to Section 793 of the Espionage Statutes, there is no definition of "intent," "reason to believe," "damage" or "advantage" in the guilt criterion. Although 793 is adequate to convict a person guilty of espionage, its applicability to a person who publishes defense information is less clear.[55] Professor Benno C. Schmidt, Jr., an authority on the Espionage Statutes, sums up his study of them as follows:

> In my reading of the Espionage Statutes, publication of defense information not animated by a purpose to communicate to a foreign country is not prohibited, except for the narrow range of cryptographic information covered by Sections 952 and 798. This reading admittedly makes heavy use of legislative history in construing the culpability provisions of subsections 794(b), 793(a) and 793(b). My conclusion rests also on the belief--perhaps speculation would be a better word--that courts will refuse to apply Sections 793(d) and (e) to acts preparatory to publication, either by finding some very narrow reading that conforms the provision to the pattern of the other Espionage Statutes, or--preferably as it seems to me--by striking the provisions from Title 18 on grounds of vagueness and overbreadth.[55a]

It is noteworthy that the United States did not invoke the Espionage Statutes against the New York Times in connection with the publication of the "Pentagon Papers."

In addition to the defects described above, the Espionage Statutes have two other major weaknesses when viewed in terms

of the protection of intelligence information, and in particular, the sources-and-methods information of CIA. First, the meaning of "defense information" contained therein is probably not broad enough to embrace the whole of sources-and-methods information or much of foreign relations information. In Gorin v. the United States, the Court declared: "In short, the phrase 'information connected with National Defense' as used in the context of the Espionage Act, means broadly, secret or confidential information which has its primary significance in relation to the possible armed conflicts in which the nation might be engaged."[56] Second, proving in a court of law "intent or reason to believe" that the information in question was to be used to the "injury of the United States, or advantage of a foreign nation" will often be more costly in terms of security than the violation to be punished. Referring to court decisions that the government must present proof of these points to a jury, the CIA Assistant General Counsel wrote: "These rulings have left the government in the position of having to reveal in court the very information it is trying to keep secret, or else not prosecute those who steal information and use it to the injury of the nation. To invoke the law's protection of the secret, the secret must be told."[57]

CONCLUSIONS AND RECOMMENDATIONS

General

Some positive steps should be taken to re-establish the credibility of the classification system. This thought is implicit in the Director's recently enunciated guiding principles for the Intelligence Community: "Improvement of the public perception of U.S. Intelligence will be given continuing attention....Within the constraints of legitimate security requirements, the Intelligence Community should strive to better public understanding of our mission and of our product....The Intelligence Community should be as responsive as possible to Congressional inquiries. Congressional support is essential to sustain the effectiveness of the U.S. intelligence effort..."[58]

A prerequisite in re-establishing the credibility of the classification system is the reduction of secrecy to an absolute minimum. This would have the effect of upgrading legitimate secrets and thereby better protecting them. "Secrecy practices which were taken for granted before Vietnam and Watergate need to be adjusted to the processes of re-establishing faith in our institutions."[59] Although some may dismiss the reduction of secrecy as merely hortatory and not very practical, it is fundamental to all reform of

the classification system. The means of achieving it are strict construction of the classification criteria in E.O. 11652, placing the burden of proof on the classifier, and, in accordance with the NSC Directive, choosing the less restrictive classification when in doubt.

In its long-standing defensive posture against the demands of Congress and the public for its closely held secrets, the executive branch has neglected to devote much attention to the theory and practice of its own classification system. Its sporadic examinations have been reactive to Congressional pressure. As a result, the only serious ongoing study of the classification system, although predominantly adversary in nature, has been done by Congress in investigative hearings.

Recommendation 1

CIA should take a leading role in the government's development of classification theory and reform of the classification system. This would promote greater Agency sensitivity to the mood of Congress and the public. This recommendation is made in full awareness that the National Security Council and the Interagency Classification Review Committee have primary responsibility in this area. The intimate connection between the classification system and the protection of foreign intelligence information justifies such an initiative. Executive Order 11905 lists as a function of the DCI

ensuring "the establishment, by the Intelligence Community, of common security standards for managing and handling foreign intelligence systems, information and products, and for granting access thereto."

Suggestions for Reform of E.O. 11652

Classification Criteria. Any radical reform of the present classification system would involve redefinition of the criteria for each level of classification. The vagueness of the criteria has been a primary source of system abuses. A study of the definitions employed throughout its history shows a gradual evolution toward greater specificity. (See Annex A.) The NSSM 229 group studying the classification system has thus far been unable to improve the current criteria for the three levels. It is true, of course, that no conceivable recasting of the criteria will ever totally remove the judgmental element from the act of classification.

On the other hand, there is nothing sacrosanct about the three present levels of classification. At one point there was only one classification--Confidential--and, at other times, there have been as many as four. Some have recommended scrapping the three existing levels and substituting a single new category, Secret Defense Data. Tinkering with the three present levels, which have existed for some twenty-five years, is more likely, however, to generate confusion than reform.

In the first place, it would be costly, it would require giving maximum protection to all information and conducting full background investigations (now only required for Top Secret) on all those granted access to the single level. And it would have a disruptive effect on agreements with our Allies in which the three levels have been incorporated.[61]

Recommendation 2

Revise the first sentence of section 1 of the Order as follows:

a. "Official information or material which requires protection against unauthorized disclosure in the interest of the national defense, foreign relations of the United States, or the protection of foreign intelligence sources and methods (hereinafter collectively termed "national security") shall be classified in one of three categories..." (The addition is indicated by underlining.)

b. An attempt should be made to cite under the criteria for each level of classification one or two telling examples of what should not be classified at that particular level, chosen on the basis of frequent and flagrant misclassification.

c. Under the criteria for Confidential, of what Confidential is, examples should be provided.

Administrative Privacy. A frequent cause of over- and unnecessary classification is the bona fide desire to protect information falling generally in the category of "administrative privacy." There is no question about the desirability of protecting this type of information if the government is to go about its business, but this information has nothing

to do with national security as defined in E.O. 11652 and should not be classified thereunder. Such information is amply protected from disclosure by the exemption provisions of FOIA and, in certain specific respects, by Sections 5 and 6 of the CIA Act of 1949.

Recommendation 3

a. Insert in Section 4 of E.O. 11652 dealing with abuses of classification a warning against the classification of information falling in the category of "administrative privacy" and reference the pertinent provisions of the FOIA and the Privacy Act.

b. In the interest of unformity and avoidance of misclassification, consideration should be given to the issuance of an Executive order or NSC directive dealing with administrative privacy and prescribing a uniform marking for this type of material (Internal Use Only, Administrative Use Only, etc.) dissimilar to present national security markings. It should reference the relevant exemptions of the FOIA.

c. Insert a caveat in the first pargraph of Section 4 of the Order warning that no information, regardless of national security considerations, may be classified if the activity it protects contravenes the U.S. Criminal Code, a statute or an Executive order.

Monitoring the Effectiveness of the Classification System.

Section 7 of the Order provided for the establishment of the ICRC to assist the National Security Council in monitoring the classification system. The Committee consists of representatives of the seven principal agencies, including CIA, concerned with classification. It has a permanent staff of eight persons. By and large the Committee has been ineffective in preventing abuses of classification and has not provided dynamic leadership to the executive branch in the field of classification theory and practice. This is no fault of the members, but rather of the part-time nature of the assignment, of the heavy responsibilities each member continues to exercise in his parent organization, and of the inability of the members to act independently of the organizations they represent.[62] The NSC directive implementing E.O. 11652 imposed on the classifying departments and agencies the onerous task of forwarding to the ICRC five types of quarterly reports. Whatever utility these reports may have, one annual report would probably provide it. There is need for a strong independent body in the executive branch to monitor the classification system and the codeword compartments.

Recommendation 4

Amend Section 7 of the Order and Section IX of the Directive as follows:

Abolish the ICRC and establish in its place a quasi-judicial board with investigative powers. Its membership would consist of senior officers from the Departments of State, Defense, and Justice, the Energy Research and Development Administration, the Central Intelligence Agency, the National Security Council Staff, and a chairman designated by the President. The members would serve for at least two years, and would not represent their parent organizations. The Board, responsible only to the NSC, would have cognizance in all matters relating to security classification, and the FOIA and the Privacy Act as they impinge on the classification system.

Special Departmental Arrangements. Section 9 of the Order authorizes originating departments to impose special requirements with regard to access, distribution, and protection of classified information. This is the charter for the codeword compartments and the plethora of dissemination and other controls that have proliferated in the Intelligence Community. Where these arrangements have repercussions beyond the originating department (as is generally the case), there should be some form of central supervision and control over departmental initiatives. Their inhibiting effect on the flow of information is imcomparably greater than that of simple classification.

Recommendation 5

Amend Section 9 of the Order and VI F of the Directive to require the concurrence of the Director of Central Intelligence whenever an NFIB member establishes a compartment

that inhibits the flow of information to other members of the Intelligence Community.

Sanctions for Noncompliance with the Order

Historically, the principal shortcoming of the classification systems has been the lack of credible, deterring sanctions against abuses and unauthorized disclosure. This explains the repetitive nature of the criticisms aimed at the various systems. Still, we are forced to the conclusion that, by and large, the proximate cause of the failure of the sanctions prescribed by the Order to deter abuses is not so much the weakness of the penalties, as their sporadic imposition.

As far as overclassification is concerned, we have seen that the system is tilted in favor of overclassification. If management wishes to, however, it should not be more difficult to make people classification-conscious than cost-conscious.

One Agency critic of the Order has charged that undue importance is given to the number of persons authorized to classify. This has had the effect of forcing busy, higher-level people to make decisions that they do not have time to make. They, therefore, accept uncritically the decisions of subordinates. He sees in this a "forced pattern of non-compliance."[63] The rationale behind limiting the number of classifiers was to reduce the amount of classified paper. As noted, this has had little effect on the volume of

classification material within the Agency. Consideration should perhaps be given to increasing selectively the number of classifiers in certain components, but only as part of an overall revamping of classification practices.

Recommendation 6

Add to Section 13(A) of the Order a requirement that supervisors rate all classifying officers on their knowledge and exercise of the classifying function. It is recommended that CIA adopt this practice independently.

CIA Management of Classification

In the section dealing with the functioning of the classification system within CIA, certain abuses, anomalies, and nonconformity with certain provisions of E.O. 11652 were noted. The interaction of FOIA and the Privacy Act with the classification system was also examined. Although no evidence was found of the use of classification to conceal inefficiency or administrative error, various investigations of the Agency, internal and external, have shown that classification served in some instances to conceal illegality, often perceived as such only retrospectively. There has emerged from the investigations what might be termed the doctrine of the "valid secret." To be valid, a secret, even if properly classified in accordance with the national security criteria, must not be tainted by

illegality, which has the effect of nullifying the classification. As remedial steps in countering CIA noncompliance with the Order, eight steps under the recommendation below are offered.

Recommendation 7

To correct the abuses, to provide centralized direction of classification and related matters, to monitor compliance with E.O. 11652 in the future, and to develop a body of doctrine, it is recommended that a CIA Classification Board, with the following features be established:

a. A five-member board of senior officers directly responsible to the Deputy Director of CIA. The members would serve full-time for tours of at least two years. Each Directorate would name a member; the chairman would be appointed by the DCI. The members would not represent their parent organizations, nor be answerable to them for their decisions.

b. The Board would have investigative, adjudicatory, and research functions within the limits of its responsibilities.

c. The Board would replace the present CIA Information Review Committee.[64]

d. Besides monitoring compliance with E.O. 11652, the Board would provide policy guidance to the office dealing with FOIA and the Privacy Act, to the Special Security Center, and to the Systems Classification Branch in the Office of Joint Computer Services. It would monitor the operation of the codeword compartments within CIA. Its concurrence would be required on the establishment of

any compartment, control, or marking affecting the flow of information beyond the originating Directorate.

e. The Board would prepare handbooks, and guides on classification, declassification, sanitization, and decompartmentation as these matters fall within the province of CIA.

f. The Board would serve as a central clearing office for information on formal and informal compartmentation, providing guidance to researchers and others on special clearances required to gain access to information needed to do their job. For this purpose, the Board would be briefed on every compartment existing within the Intelligence Community which is relevant to the mission of CIA.

g. The Board would be provided with a small permanent secretariat designed to provide research and secretarial support.

Recommendation 8

a. A handbook dealing with not only the basics, but also the more subtle aspects of classification, its interrelationships with FOIA and the Privacy Act, should be prepared. The ERDA handbook on classification could serve as a model.

b. There is need to establish training programs on classification, FOIA, and the Privacy Act, especially for original classifiers. A program of periodic reorientation of employees on classification, as required by the Order, should be instituted.

Recommendation 9

a. A beginning should be made on compliance with that section of the Order enjoining classification by portion or paragraph, where feasible. This would facilitate declassification and minimize overclassification in those cases where information is extracted and incorporated in other reports. (It should be noted that at the present time cabled intelligence summaries prepared by OCI are classified by paragraph.)

b. In addition to paragraph marking, an attempt should be made to devise guidelines that would permit de novo classification, under specified conditions, of information extracted from raw reports for incorporation in finished intelligence.

Recommendation 10

Top Secret cables should be handled in the same manner as other Top Secret collateral material once they leave the Cable Secretariat and should be brought under the supervision of the Top Secret Control Officer. The problem of better control of Top Secret codeword material requires further study.

Recommendation 11

Pre-printed forms marked: Secret When Filled In, are a prime cause of overclassification. They should be abolished and replaced with forms that offer other classification options, including Unclassified.

Recommendation 12

There should be a thorough review, at least annually, of the number and level of classifiers required by each component. Both the tables of organization upon which the allocation of original classifiers is usually based and the lists of authorized classifiers appear in need of updating. Selective increases in the number of classifiers seem warranted in some components. These increases could probably be offset by removing from the lists those who exercise their classification authority infrequently or not at all. To dispel confusion in the minds of many officers, those authorized to classify should be reminded of the level at which they are authorized to classify at least annually and those whose authorization has been terminated should be notified immediately.

Recommendation 13

A regulation should be issued on the handling of information falling in the category of "administrative privacy." It should reference the pertinent provisions of FOIA and the Privacy Act. It should prescribe uniform marking and protection for this information, emphasizing that it should not be classified under E.O. 11652 unless it has unmistakable claims to this protection in terms of national security and/or the protection of sources and methods. (Section 8f of CIA Regulation [redacted], dealing with dissemination controls

for foreign intelligence, lists as additional controls: CIA Internal Use Only, Administrative-Internal Use Only, and For Official Use Only. Administrative-Internal Use Only, which comes closest to a marking for administrative privacy, is defined as a control that may be used "for unclassified, non-sensitive administrative information that should not be disseminated outside of CIA." If this definition were broadened to include the types of unclassified information exempted by the FOIA and if protective measures were prescribed, this control would satisfy the sense of this recommendation.)

Recommendation 14

To bring the current exponential proliferation of classified paper through Xeroxing under control, research should be conducted into the feasibility of a system similar to the following: Programming the Xerox copying machine so that it will not function unless certain information is input into it--the name or badge number of the employee, whether the document to be copied is unclassified or draft and, if classified, the classification, subject, dispatch symbol, etc. If classified, (the machine could be programmed to recognize this from the marking), the machine could assign a control number and provide a record of copies made. Something of this sort should serve two purposes: deter Xeroxing and, where necessary, provide an inventory of classified documents that have been Xeroxed.

The Problem of Disclosure

This Study has examined the statutory and constitutional barriers to disclosure--the Espionage Statutes, executive privilege, the classification system, certain provisions of FOIA and the Privacy Act, the sources-and-methods clause--and found them wanting in important respects. Before suggesting any remedies, it is first necessary to consider various proposals that have been made for a statutory solution.

During the last Senate hearings on classification in 1974 there were six bills pending before Congress designed to create a statutory classification system.[65] The motivation behind these bills was not to give greater protection to government secrets by providing legal underpinning but rather, through various devices, to accelerate the declassification of information and insure Congressional access to executive branch secrets. One bill (S. 1520) would set up a National Committee on Executive Secrecy; another (S. 3399) would create a Classification Review Commission. In the case of the latter, Congress would propose the names of six of the nine members to the President for appointment. This thinly veiled intent to share executive power is probably unconstitutional. The proposed Classification Review Commission would be empowered to overrule the President on classification matters. As mentioned above, two bills

(S. 1726 and S. 2451) would set up a single classification--Secret Defense Data--that S. 2451 defines as information the unauthorized disclosure of which "would adversely affect the ability of the United States to protect itself against overt or covert hostile action." The bills generally avoid the "national security" formulation of E.O. 11652 in favor of an undefined "national defense." None was found satisfactory by the executive branch, and none contains features that would be helpful in drafting a constructive statutory vehicle for the classification system.

More deserving of our attention is Subchapter C, Chapter 11 of S.1, a Senate bill entitled "The Criminal Justice Reform Act of 1975." This subchapter, a part of a monumental codification of Federal criminal law, over twenty years in the making, presents a revision of the Espionage and related statutes discussed earlier. Sections 1121-1123 deal with espionage and the disclosing and mishandling of "national defense information." Section 1124 penalizes the disclosure to an unauthorized person of any type of classified national defense information. The vague "intent or reason to believe" wording of Sections 792-794 of the Espionage Statutes has been replaced throughout Subchapter C by the following guilt formulation: "knowing that defense information could be used to the prejudice of the safety or interest of the United States, or to the advantage of a foreign power."

A key element in the codification of these statutes is the definition of "national defense information" in Section 1128(f). The latter is essentially an enumeration of ten types of information, the first five of which relate to military secrets. Item (6) reads: "intelligence operations, activities, plans, estimates, analyses, sources, or methods, of the United States." The remaining four specify intelligence concerning a foreign power, communications intelligence and cryptographic information, atomic Restricted Data, and any matter involving the security of the U.S. in time of war.

Section 1123 would indirectly permit the prosecution of anyone deliberately publishing national defense information, but the burden of proof would be upon the government to convince the jury that the information was in fact national defense information. Thus, we are faced again with the dilemma encountered earlier, the requirement of proof that would compound the damage already done to national security.

Although Section 1224 embraces "all" classified information and applies to former as well as present government employees, it specifically exempts from prosecution the unauthorized person to whom national defense information has been communicated. Since the unauthorized recipient may well be a member of the press, Section 1124 is not an effective deterrent to the publication of classified information.

Moreover, by bringing Section 798 of the Espionage Statutes (the section protecting communications intelligence, etc., and the most effective of the Espionage Statutes) under its wing, Section 1124 vitiates 798.

In short, Subchapter C represents an advance in terms of simplicity of language, procedure, and careful definition of terms, but a step backwards in exempting from prosecution the unauthorized recipient of classified information and in using the concept, "national defense information," rather than that of "national security information." Foreign relations information, an essential element of the latter, is apparently excluded from its purview.[66]

Those who decry the lack of effective statutory deterrents to disclosure often look enviously at the British Official Secrets Act. The latter, however, with its D-notices and catchall language that protects any "official information" whether related to national security or not, is not only inconceivable politically in the context of American freedoms but would undoubtedly be struck down by the courts as unconstitutional.[67]

Recommendation 15

The Agency should propose legislation along the following lines to protect sources-and-methods information. The proposed legislation should be patterned on the Atomic Energy Act of 1954. It should:

a. amend section 102(d)(3) of the National Security Act of 1947 for the purpose of defining sources and methods and creating a new category of legally protected information, overlapping with but independent of the classification system.[68] Like Restricted Data, Foreign Intelligence Data or Sources and Methods Information would be "born classified."

b. reference exemption (b)(3) of the Freedom of Information Act.

c. provide for an energetic program of removal of nonsensitive or sanitized sources-and-methods information from the special category to the protection of simple classification, or, if appropriate, declassification. These procedures would usually apply to the product of sources and methods and, only rarely, to sources and methods per se. There is a partial analogy to Formerly Restricted Data.

d. prescribe a full background investigation as a condition of access to sources-and-methods information.

e. make clear that the proposal is not directed against Congress and that all appropriate information will be made available to concerned committees of Congress in secret session. There has been no known leak of Restricted Data by Congress and hopefully the same would be true of sources-and-methods information.

f. ban all controls, markings, or compartments, other than the three levels of classification, within the Foreign Intelligence Data category, unless approved by the DCI. In general, supplementary protection, other than through a strict application of need-to-know, should be unnecessary within the special category.

Where applicable, the three levels of classification of E.O. 11652 should continue to be utilized within the special category. By definition, however, sources-and-methods information would be protected, whether classified or not.

Recommendation 16

The DCI, acting within the NFIB structure, should designate an ad hoc committee of legal experts to study the revision of the Espionage Statutes. In particular, sections 792 through 796 should be consolidated, simplified, and clarified. The intent criteria should be abolished and other loopholes plugged. As an alternative to Recommendation 15, section 798 dealing with cryptographic information could be expanded to include sources-and-methods information, or a separate section could be added for this purpose. (Because of its primary responsibility in this area, the establishment of such a committee would, of course, have to be closely coordinated with the Justice Department.)

FOOTNOTES

1. The dictionary defines compartmentation as division into separate sections or units, giving as an example, the elaborate compartmentation of submarines which reduces the danger of sinking. Within a government agency, and particularly within an intelligence organization, compartmentation takes on a special coloration. In this context, it may be defined as the deliberate restriction of the free flow of information for the purpose of minimizing the risk of unauthorized disclosure of designated types of information whose protection is deemed essential to the organization.

One may picture compartmentation as a series of rings starting with the badge that excludes those who are not members of the organization, and working inward and upward through the levels of document classification to the ever smaller rings of the codeword compartments. If the application of compartmentation were absolute in the sense of the submarine analogy, the organization would suffocate. What enables the organization to survive is the operation of the countervailing principle of "need-to-know" permitting a directed flow of information.

Interacting with deliberate compartmentation are various bureaucratic practices that tend to clog the need-to-know channels and magnify difficulties in the compartmented systems. In the series of Center studies, compartmentation has been viewed as "formal" as it relates to the codeword systems, "informal" as it pertains to the generalized need-to-know found in the classification system or the more rigid need-to-know practiced in the Clandestine Service, and "bureaucratic" as it evolves accidentally from organizational phenomena. Forthcoming studies in this series will deal with formal and bureaucratic compartmentation as well as other aspects of informal compartmentation.

2. A unique source of information on the pre-World War II origins of the classification system is a typescript by Dallas Irvine, Origins of Defense-Information Markings in the Army and Former War Department. Washington: National Archives and Records Service, 1972. Particularly valuable are the appendices to this work reproducing the original documents referred to in the text. An excellent overall view is given by Harold C. Relyea, "The Evolution of Government Information Security Classification Policy: A Brief Overview (1775-1973)." It appears as a supplement in: Government Secrecy: Hearings before the Subcommittee

on Intergovernmental Relations of the Committee on Government Operations...on S. 1520, S. 1726, S. 2451, S. 2738, S. 3393, and S. 3399. May 22, 23, 29, 30, 31, and June 10, 1974. Washington: U.S. Govt. Print. Office, 1974. The following two works cover much the same ground, but are useful for recent developments and bibliographic references: William G. Phillips. "The Government's Classification System." Ch. 2 in None of Your Business-Government Secrecy in America. Ed. Normal Dorsen and Stephen Gillers. New York: The Viking Press, 1974; Representative William S. Moorhead. "Operation and Reform of the Classification System in the United States." Ch. 6 in Secrecy and Foreign Policy. Eds. Thomas M. Franck and Edward Weisband. New York: Oxford University Press, 1974.

3. Other changes effected by E.O. 11652 are summarized in Annex B.

4. Quoted in H. Rept. 93-221, Executive Classification of Information-Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act (5 U.S.C. 552). 93d Congress. 2d Sess. Washington: U.S. Govt. Print. Office, 1973, p. 16.

5. Quoted by Relyea, op. cit., p. 861.

6. Ibid., pp. 875-876. For the text of the proposed bill see Appendix III of Relyea's study. Appendix II contains the text of other recommendations.

7. Quoted by Relyea, ibid., p. 863.

8. Ibid., pp. 863-865.

9. Moorhead, op. cit., p. 98.

10. Ibid., pp. 77-78. See also H. Rept. 93-221, op. cit., Ch. VI, and Senate Hearings on Government Secrecy, op. cit., passim.

11. Moorhead, op. cit., pp. 100-101.

12. Phillips, op. cit., pp. 72, 96, 101. Dr. Ray S. Cline, testifying at the 1974 Senate hearings estimated that "there probably is 15 to 25% of the material that is classified by the Government which, at least at the time, is legitimately classified." Senate Hearings on Government Secrecy, op. cit., p. 56.

13. Stanley Futterman. "What is the Real Problem with the Classification System?" Ch. 3 in None of Your Business, op. cit., p. 103.

14. Quoted by Phillips, op. cit., p. 69.

15. [redacted]. "Secrecy and Intelligence in a Free Society," an unpublished study done for the Center for the Study of Intelligence. Some of the highlights of this study appear in: "Secrecy and Intelligence in a Free Society-The Dilemma of Security vs. Openness," Studies in Intelligence. Vol. 19, No. 2, summer 1975.

16. Quoted by William G. Florence. "Issues in Classifying and Protecting National Defense Information." Ch. 10 in Surveillance and Espionage in a Free Society. Ed. Richard H. Blum. New York: Praeger Publishers, 1972, p. 132.

17. [redacted] op. cit., pp. 91-92.

18. Florence, op. cit., p. 132.

19. Apposite description used by Dr. Edward Proctor in a talk to the Senior Seminar on 3 May 1976.

20. [redacted] op. cit., pp. 9-10.

21. During the period 1 January 1973 to 31 March 1974, there were 33 recorded abuses of classification in CIA, 26 of which were attributable to overclassification and two to unauthorized disclosure, source unknown. The reprimands given were characterized as more educational than punitive in tone and were not entered in personnel files. Colby Letter to Senator Edmund S. Muskie, 24 May 1974. Senate Hearings on Government Secrecy, op. cit., pp. 114, 469.

22. A memorandum from the chairman of the ICRC, dated 22 March 1976, to the departments authorized to classify information under E.O. 11652 stresses that the use of such designations as "Top Secret/Sensitive," "White House Confidential," and "Conference Confidential" is a violation of the Order and should be discontinued.

23. Senator Muskie used a figure of 96% for the amount of CIA information exempted. Senate Hearings on Government Secrecy, op. cit., p. 102. Commenting on this at a later date, he remarked: "That is to say the Executive order is a

dead letter in its application to that institution." Ibid., p. 252. At the same hearings the following exemption figures for other agencies were given: FBI, over 99%; Defense Department, 50%; State Department, less than 50%. Ibid., p. 162.

24. CIA Annual Report to the Congress for the Year 1975 on the Freedom of Information Act.

25. Ibid.

26. See Edward A. Shils, The Torment of Secrecy, New York: Free Press, 1956, for a sociological analysis of this triad.

26a. In 1974 the Office of the Inspector General conducted a review to determine "whether Agency officers with classification authority understand classification criteria and are complying with guidance...." In pursuing this objective, the review did not consider "substantive intelligence" nor cable traffic, limiting itself essentially to "administrative material." The principal conclusions of its four-page report were these:

- The Agency has made progress in responding to E.O. 11652. There is "more discretion in classification decisions."

- There is some overclassification in the Agency, but it is "not a problem of any serious magnitude." Much remains to be done, however, in correcting the overclassification of pre-printed forms. And, the report adds, "given the nature of the Agency's business, the tendency to overclassify will remain with us for some time."

- In some components no distinction is made between the authority to classify and the authority to exempt.

- Training for classification officers is virtually non-existent.

- There is apparently no periodic review of classified material for downgrading and declassification.

- The report recommends "a periodic training program" for classification officers and the designation of an officer in each component to review at regular

intervals chrono files for classification abuses. See: Memorandum For: Chief, Information Systems Analysis Staff. Subject: Classification/Declassification of Information. DD/M and S 74-1319, dated 12 April 1974.

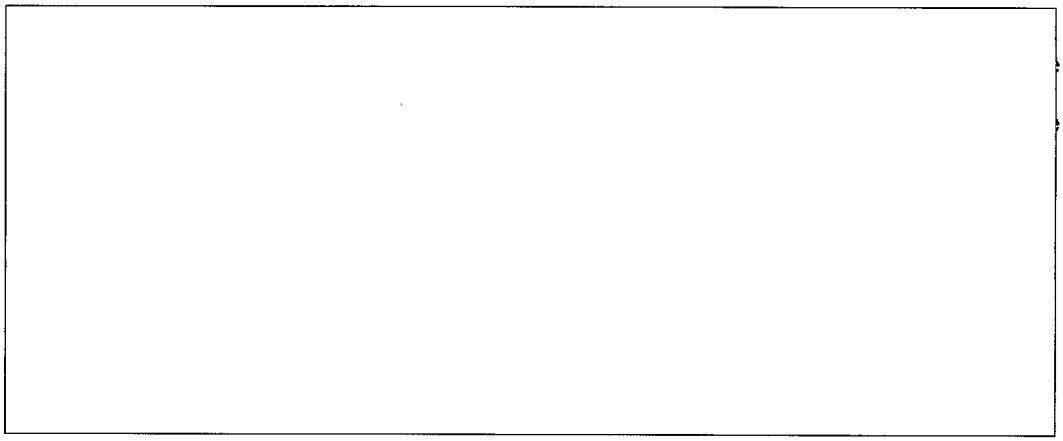
27. The National Archives and Records Service (NARS) has general supervisory responsibility for the destruction of useless official records. Each government Agency is required to provide the NARS with a records schedule setting forth the disposition of its records. Actual destruction may then be carried out by each agency in accordance with the schedule.

28. Futterman, op. cit., pp. 93-94.

29. The rationale for all forms of supplementary protection is sensitivity. The security classification system itself is a three-step sensitivity scale. Top Secret information is information requiring "the highest degree of protection." Leaving aside practical considerations such as managerial efficiency, there is obviously a logical redundancy in providing supplementary protection to Top Secret information.

30. Memorandum For: Executive Secretary, CIA Management Committee. Subject: Central Storage and Retrieval of Sensitive Intelligence Documents, 6 August 1973, p. 5 of Attachment to report entitled "Security of the CRS System."

31. Ibid., p. 3 of report.



[redacted]

33. The Rockefeller Commission Report notes: "In connection with the statutory responsibility of the Director of Central Intelligence for the protection of intelligence sources and methods from unauthorized disclosure, the National Security Council has directed that each agency or department be responsible for the protection of its own sources and methods, and that the Director call upon these other bodies as appropriate to investigate any unauthorized disclosures and report to him. The Director has, in turn, delegated these responsibilities to the Security Committee of the United States Intelligence Board [now the National Foreign Intelligence Board]..." Report to the Commission on CIA Activities within the United States. Washington: Govt. Print. Office, June 1975, p. 56. The precise extent to which the DCI's statutory responsibility extends to other members of the Intelligence Community is unclear.

34. JSSC memorandum, dated 18 September 1945, entitled "Proposed Establishment of a Central Intelligence Service. Report of the Joint Strategic Survey Committee." It references Joint Chiefs of Staff (JCS) memorandum 1181 (Donovan's recommendations). The National Intelligence Authority was the predecessor of the National Security Council.

35. JCS 1181/5 (amended). "Establishment of a Central Intelligence Service Upon Liquidation of O.S.S. Directive Regarding the Coordination of Intelligence Activities." For text see Appendix R, Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency, by [redacted] CIA, 1975 (~~SECRET~~).

36. Memorandum from Director of Naval Communications to Chief of Naval Operations, dated 8 January 1975. Subject: Establishment of a National Intelligence Service-Necessity for Safeguarding the Security of Military Intelligence in Connection Therewith.

37. This seems borne out by these words in the Central Intelligence Group (CIG) draft for the CIA section of the 1947 Act: "Be responsible for fully protecting sources and methods used in the collection of foreign intelligence information received by the Agency..." And also in the draft for a separate CIA Act of 10 March 1947: "Be responsible for taking measures to protect sources and methods used in the collection and dissemination of foreign intelligence information received by the Agency..." The Rockefeller Commission Report, op. cit., p. 53, expresses a similar view: "This language [sources and methods] was originally inserted in the early drafts of the Act in response to the expressed concern of some military officials that a civilian agency might not properly respect the need for secrecy. Congress was also aware of the concern that the United States espionage laws were ineffective in preventing unauthorized disclosure of classified information."

38. [redacted]. "The Protection of Intelligence Data." Studies in Intelligence. Vol. 11, No. 2, p. 72.

39. Letter from John S. Warner to Senator Muskie, Senate Hearings on Government Secrecy, op. cit., p. 115.

40. This definition draws on some of the concepts contained in the OGC catalog of sources and methods and the Agency-sponsored bill dealing with sources and methods. See footnotes 42 and 66. "Foreign intelligence information" itself would, of course, also require definition. The Rockefeller Commission Report observes that "'foreign intelligence' is a term with no settled meaning. It is used but not defined in National Security Council Intelligence Directives. Its scope is unclear where information has both foreign and domestic aspects." Op. cit., p. 59. It adds its belief that "...congressional concern is properly accommodated by construing 'foreign intelligence' as information concerning the capabilities, intentions, and activities of foreign nations, individuals or entities, wherever the information can be found. It does not include information on domestic activities of United States citizens unless there is reason to suspect they are engaged in espionage or similar illegal activities on behalf of foreign powers." Ibid., p. 59.

41. For a short account of this case, see: Guide to CIA Statutes and Law, p. 16. Also Lawrence R. Houston. "U.S. v. Jarvinen." Studies in Intelligence. Vol. 15, No. 1.

42. Guide to CIA Statutes and Law, pp. 16-18.

43. On this point Judge Haynsworth reiterated his previous holding "that the First Amendment is no bar against an injunction forbidding the disclosure of classifiable information within the guidelines of the Executive Orders when (1) the classified information was acquired, during the course of his employment, by an employee of a United States agency or department in which such information is handled and (2) its disclosure would violate a solemn agreement made by the employee at the commencement of his employment. With respect to such information, by his execution of the secrecy agreement and his entry into the confidential employment relationship, he effectively relinquished his First Amendment rights." Opinion, p. 15. For a brief summary of the Marchetti case prior to the final appeal see Victor Marchetti and John D. Marks. The CIA and the Cult of Intelligence. New York: Alfred A. Knopf, 1974. Introduction by Melvin L. Wulf, legal director of ACLU and Marchetti's defense lawyer. The Supreme Court refused to review the Marchetti case.

44. Backrack was suing for all information on the relations of Nicholas de Rochefort (deceased) with CIA and its predecessor organizations. Paragraph 9 of Judge Gray's opinion is particularly noteworthy: "Since it is concluded that the exemptive provisions of 5 U.S.C. 552(b)(3) [that is, the sources-and-methods provisions under the FOIA statutory exemption] are applicable herein, the Court has no occasion to consider whether the sought information, if it exists, would also be exempt from disclosure by the provisions of U.S.C. 552(b)(1) [information properly classified pursuant to an Executive order]." The other cases referred to in the text are: Harriet A. Phillippi v. CIA, et. al., 1 December 1975, a case in which in camera examination of documents with the plaintiff's lawyer present was denied; William B. Richardson v. J.T. Spahr et. al., 30 January 1976, a consolidation of three suits demanding CIA financial records; Gary A. Weissman v. CIA et. al., 14 April 1976, in which the plaintiff requested the CIA security file on himself; Jonathan A. Bennett v. DOD, CIA, et.al., 13 September 1976, requesting information on all missions sent into Cuba by DOD; and Morton H. Halperin v. William E. Colby, et. al., 4 June 1976, a request for budgetary information (Although the sources-and-methods provisions were cited by the judge, the case was decided on the basis of exemption (b)(1)); and Anthony V. Vecchiarello v. Edward Levi, et. al, (CIA), 1 June 1976. The District Court decided that the disputed information was properly withheld under the FOIA exemptions.

45. The sources-and-methods catalogue, OGC 76-03333, dated 12 December 1975, is entitled "Aspects of Intelligence Sources and Methods of the Central Intelligence Agency That Require Protection from Unauthorized Disclosure." It is divided into twelve sections with a total of 126 "aspects." Approved by the DCI on 12 January 1976, it is to be issued as an Agency regulation. An OGC staff memorandum explaining the rationale of the sources-and-methods catagloue notes that in those instances where the district court decided against the Agency's deletions from Marchetti's book, it was generally because the Agency was unable to document prior determinations concerning the classification of the contested item. The nondisclosure agreement for sources-and-methods information will be in addition to the secrecy agreement that employees now sign for the protection of classified information.

46. Shils, op. cit., p. 41. He adds: "With its [America's] devotion to publicity on such a scale, it could scarcely be expected that in its normal state Americans would have much sympathy with secrecy, particularly government secrecy." Ibid., p. 42. And again: "No society has ever been so extensively exposed to public scrutiny as the United States in the twentieth century." Ibid., p. 39.

47. Writing of the disclosures of CIA cover and funding operations in 1967, [redacted] concludes: "Habits of thinking within the Agency and the Executive had become outmoded, and preserved from change by secrecy." Op. cit., p. 64. In other words, covert operations that had been appropriate and credible in the fifties had ceased to be so in 1967, but were not recognized as such until it was too late. Secrecy often tends to breed insensitivity to change and public opinion.

48. Cited by Professor Arthur Schlesinger, Jr., Senate Hearings, op. cit., pp. 40-41.

49. The preamble to E.O. 11652 takes note of the section of the Freedom of Information Act (552(b)(1) of Title 5, U.S.C.) exempting properly classified information from disclosure, but the Executive order does not expressly derive its authority from that Act.

50. Quoted by Stanley Futterman. "What is the Real Problem with the Classification System?" Ch. 3 in None of Your Business, op. cit., p. 102.

51. Speaking of the decision in the "Pentagon Papers" case, New York Times v. United States, Ralph E. Erickson, then Assistant Attorney General, expressed this view: "While the Justices applied a number of different standards, it seems clear that injunctive relief against publication of classified material already in the hands of the press will be granted only in the most extreme circumstances, at least in the absence of specific legislation." Hearings on the Proper Classification and Handling of Government Information Involving the National Security and H.R. 9853, a Related Bill. Special Subcommittee on Intelligence. House Armed Services Committee. 92d Congress. 2d Sess. March and May 1972. H.A.S.C. No. 92-79, p. 17472.

52. The then Atomic Energy Commission (AEC) Classification Handbook and excerpts from the Atomic Energy Act are reproduced in the Senate Hearings on Government Secrecy, op. cit., pp. 364-467.

53. The House Committee Report on Executive Classification, op. cit., p. 99, makes this interesting comment on the atomic energy program:

> Like other executive agencies the AEC also functions within the Executive order classification system, as well as its own statutory system. The committee notes, however, the sharp contrast between the apparent efficient operation of the AEC classification system and the administrative failures that have marked the operation of the Executive order system within the past 20 years.
>
> It is true that the highly technical type of information that is subject to classification within AEC's own statutory system and its limited scope of applicability makes it more manageable. Moreover, scientific development in the atomic energy field usually provides more precise benchmarks for measuring the necessity to continue classification of AEC information at a particular level than is generally true in the fields of foreign policy or defense information.

54. Benno C. Schmidt, Jr. "The American Espionage Statutes and Publication of Defense Information." Ch. 11 in Secrecy and Foreign Policy, op. cit., p. 188. By dropping the word "intent" and retaining "reason to believe" and by substituting for foreign person or power "any person not

entitled to receive it," subsections (d) and (e) of 793 come closest to embracing press disclosure of defense information. Subsection (d) prescribes penalties for one lawfully in possession of defense information who refuses to deliver it on demand to an officer or employee of the United States "entitled to receive it"; subsection (e) covers a person who, being in unauthorized possession of defense information retains it, communicates it to another unauthorized person, or refuses to surrender it to an officer or employee of the United States entitled to receive it. Prior to 1950 there was only a section (d) applying to government employees; the addition of (e) was done as a result of the Whittaker Chambers "pumpkin papers" case to criminalize retention by non-goverment personnel. Ibid., p. 188.

55. Ibid., p. 198. The present Espionage Statutes comprise in the main legislation enacted in 1911, 1917, and 1950. The most recent provision, Section 799, deals with the protection of NASA secrets.

55a. Ibid., p. 201. Section 952 (18 U.S.C. 952) imposes penalties on a government employee who publishes or makes unauthorized disclosure of information concerning or transmitted by a foreign diplomatic code.

56. Quoted in CIA publication entitled "Title 18, U.S. Code. Sections 792, 793, 794, 795, 796, 797, and 798 with an Interpretation of the Internal Security Act of 1950." p. 6.

57. [redacted] op. cit., p. 75. Mention should also be made of another statutory barrier to disclosure, subsection (b) of the Internal Security Act of 1950 (50 U.S.C. 783). This subsection makes it a crime "for any officer or employee of the United States" to communicate to a foreign agent "any information of a kind which shall have been classified by the President as affecting the security of the United States..." Quoted by Ralph E. Erickson in statement to the House Subcommittee on Intelligence, H.A.S.C. No. 92-79, op. cit., p. 17471. It apparently does not apply to former government employees.

58. Guiding Principles for the Intelligence Community, 13 May 1976. NFIB-D-1/49.

59. [redacted] op. cit., p. 10.

60. See Senate bills S. 1726 and S. 2451. Texts and analysis of these and other bills dealing with classification

will be found in Legislation on Government Secrecy. Subcommittee on Intergovernmental Relations. Committee on Government Operations. U.S. Senate. Washington: Govt. Print. Office, 1974. Florence, a strong protagonist of a single-tier system, wrote, op. cit., p. 131: "Consistent with the urgent need for narrowing the scope of any executive order or law for the protection of national defense information, there should be only one category of such information. Internal distribution designators could be used to limit the dissemination of a given item, but there should be only one classification marking to indicate the application of law or, in the absence of law, such an executive order as might exist."

61. See testimony of Fred Buzhardt, General Counsel, Department of Defense, before House Subcommittee on Intelligence, op. cit., pp. 17376-17377 and that of William Blair, Deputy Assistant Secretary of State, ibid., pp. 17562-17464. The Rehnquist Committee considered and rejected suggestions for both a one-tier and a two-tier classification system.

62. "The ICRC is charged with duties it cannot perform, given the size of the staff and the volume of non-ICRC duties of its members. Realistically, it is not possible to allocate sufficient resources (money and people) to provide the necessary expertise and support services. Further, conceptually, a Committee of departmental employees cannot monitor and regulate the policies and practices of the heads of their own departments." Memorandum to ICRC Chairman, dated 9 March 1976, from CIA member [redacted] OGC-76-1148. The memorandum is entitled: "Issues and Problems with Executive order 11652."

63. Ibid.

64. The CIA Information Review Committee consists of the DDA, who is the chairman, the DDI, the DDO, the DDS&T, the Deputy for National Intelligence, and the General Counsel. It is obvious that a high-level body such as this, which also handles FOIA appeals, can only address itself to the most urgent problems posed by the classification system and not to radical reform of the latter.

65. See Legislation on Government Secrecy, op. cit.

66. See S. 1, Chapter 11, Subchapter C, pp. 68-74. The bill is dated 15 January 1975. See also Report of the

Committee on the Judiciary United States Senate to Accompany S.1, 94th Congress, 1st Sess., Rpt. No. 94, Washington: U.S. Govt. Print. Office, 1975, particularly pp. 229-263. Sub-chapter D takes over the provisions of the Atomic Energy Act, as amended, but does not appear to weaken them. The National Commission that worked on the codification of Federal criminal law used the term "national security information" which the Judiciary Committee replaced with "national defense information."

67. D-Notices are administrative warnings by the Defense, Press and Broadcasting Committee that information someone proposes to publish is secret and concerns national security. For a discussion of the Official Secrets Act see Franck and Wiesband, op. cit., pp. 325-331. [redacted] op. cit., pp. 70-71, explains that the British acts "are based on the theory of privilege, according to which all official information, whether or not related to the national defense and security is the property of the crown. It is therefore privileged, and those who receive it officially may not divulge it without the crown's authority." And he concludes: "In short, the Official Secrets Acts would seem to be in important respects unconstitutional in this country and therefore cannot be relied on as examples of means by which we could protect intelligence data." Ibid., p. 72.

68. An Agency-sponsored bill, H.R. 12006, introduced by Representative Robert McClory on 19 February 1976, aims at strengthening the sources-and-methods clause by adding a new subsection (g) to Section 102 of the National Security Act of 1947. Its main features are these:

--It criminalizes the communication of classified sources-and-methods information to an unauthorized person or the general public.

--It extends to anyone who is or has been in authorized control or possession of classified sources-and-methods information, but not to the unauthorized recipient of such information.

--It requires in camera hearings when a court wishes to determine whether the information was properly classified and designated as sources-and-methods information (the court's determination is then a point of law).

--It provides for a temporary or permanent injunction when in the judgment of the DCI a violation is

imminent. Unless there is presumptive evidence of improper classification, the court is directed not to hold an in camera hearing prior to granting an injunction.

Information relating to sources and methods is defined as "any information, regardless of its origin, that is classified pursuant to the provisions of a statute or Executive order, or a regulation or a rule issued pursuant thereto as information requiring a specific degree of protection against unauthorized disclosure for reasons of national security and which, in the interest of the foreign intelligence activities of the United States, has been specifically designated by a department or agency of the United States Government which is authorized by law or by the President to engage in foreign intelligence activities for the United States as information concerning--(A) methods of collecting foreign intelligence; (B) sources of foreign intelligence, whether human, technical, or other; or (C) methods and techniques of analysis and evaluation of foreign intelligence."

According to the Office of the General Counsel, the Justice Department insisted on the provision in the bill restricting protected sources-and-methods information to that which has been classified.

The bill's exemption from prosecution of the unauthorized recipient of sources-and-methods information was apparently inspired by similar language in Section 1124 of S.1 (dealing with classified national defense information). Because of this exemption, H.R. 12006 affords considerably less protection to sources-and-methods information than Section 798 of the Espionage Statutes (also limited to classified information) affords to communications intelligence.

By limiting sources-and-methods information to that which has been classified it tends also to undercut the theory that sources-and-methods information has statutory claims to protection under Section 102(d)(3), independent of the classification system. Unlike the Atomic Energy Act, this bill does not create a unique category of information that is "born classified."

On the other hand, it breaks new ground in the statutory protection of information with its provisions for unjunctive relief and in camera hearings. The injunctive provision could apparently be invoked against a newsman who planned to publish sources-and-methods information, but the newsman would not be actionable under the provisions of the bill if he managed to publish the information before being restrained.

ANNEX A

A SELECTION OF CLASSIFICATION CRITERIA*

(Arranged Chronologically)

21 November 1907. Circular No. 78, War Department.

Paragraph 1 of the Circular specified that Confidential is permitted only "where the subject matter is intended for the sole information of the person to whom addressed." Paragraph 2 required that issuances be accompanied by a statement indicating the class or classes of individuals to whom the contents might be disclosed. Paragraph 4 stated that issuances marked Confidential in the past were for the use of Army officers, enlisted men, and government employees "when necessary in connection with their work." (Irvine, op. cit., p.14.)

British Classification Criteria

The criteria are based on the degree of damage which disclosure would entail:

Top Secret--"exceptionally grave damage to the nation."

Secret--"serious injury to the interests of the nation."

Confidential--"prejudicial to the interests of the nation."

Restricted--"undesirable in the interests of the nation."

(Franck and Wiesband, op. cit., p. 336.)

*Full identification of the references cited after each entry will be found in the footnotes.

21 November 1917. General Orders, No. 64, General Hqrs., AEF.

General Orders, No. 64, General Headquarters, American Expeditionary Force, established three classifications for "official information."

Confidential: "Confidential matter is restricted for use and knowledge to a necessary minimum of persons, either members of this expedition or its employees."

Secret: "The word 'secret' on a communication is intended to limit the use or sight of it to the officer into whose hands it is delivered by proper authority, and, when necessary, a confidential clerk. With such a document no discretion lies with the officer or clerk to whom it is delivered, except to guard it as SECRET in the most complete understanding of that term. There are no degrees of secrecy in the handling of documents so marked. Such documents are completely secret."

For Official Circulation Only: "Orders, pamphlets of instruction, maps, diagrams, intelligence publications, etc., from these headquarters...which are for ordinary official circulation and not intended for the public, but the accidental possession of which by the enemy would result in no harm to the Allied cause; these will have printed in the upper left hand corner, "For Official Circulation Only."

This order also prescribed the following circulation controls:

Not To Be Taken into Front Line Trenches; Not To Be Reproduced; Not To Go Below Division Headquarters; Not To Go Below Regimental Headquarters. (Irvine, op. cit., pp. 24-25. The markings, "Secret" and "Confidential," were borrowed from the French. The British had a marking "For Official Use Only."

14 December 1917. Compilation of Orders, No. 6, War Department

Section 176 of the Compilation of Orders reads:

> A document or map marked 'Secret' is for the personal information of the individual to whom it is officially entrusted and of those officers under him whose duties it affects. The officer to whom it is entrusted is personally responsible for its safe

custody and that its contents are disclosed to those officers mentioned above, and to them only. The existence of such a document or map will not be disclosed by the officer to whom it is entrusted, ..."

"A document or map marked 'Confidential' is of less secret a nature than one marked 'Secret,' but its contents will be disclosed only to persons known to be authorized to receive them or when it is obviously in the interest of the public service that they receive them."

"The information contained in a document or map marked 'For Offical Use Only' will not be communicated to the public or to the press, but may be communicated to any person known to be in the service of the United States simply by virtue of his official position."

Section 176 also required that catalogues of classified documents be classified. (Irvine, op. cit., Appendix K.)

22 January 1921, Army Regulations, 330-5.

"A document will be marked 'Secret' only when the information it contains is of great importance and when the safeguarding of that information from actual or potential enemies is of prime necessity.

A document will be marked 'Confidential' when it is of less importance and of less secret nature than one requiring the mark of 'Secret,' but which must, nevertheless, be guarded from hostile or indiscreet persons.

A document will be marked 'For Official Use Only' when it contains information which is not to be communicated to the public or to the press, but which may be communicated to any person known to be in the service of the United States whose duty it concerns, or to persons of undoubted loyalty and discretion who are cooperating with Government work." (Irvine, op. cit., pp. 33-34.)

12 February 1935, Changes No. 3 in Army Regulations, 850-25.

A fourth classification "Restricted" was added.

"Whenever the chief of an arm or service which is charged with a research project or design, development, test, and production of a unit of military equipment or component thereof, shall determine that the maintenance of secrecy regarding any such project is sufficiently important to the national defense of the United States to warrant it, he may declare it a 'Restricted' project. Information regarding a 'Restricted' project will be considered to be information affecting the national defense within the meaning of the provisions of the Espionage Act (sections 1 and 2, Title I,..." "During the period that a project has a restricted status, all documents...containing technical information regarding it will be identified by being marked substantially as follows: Notice This document contains information affecting the national defense of the United States within the meaning of the Espionage Act (U.S.C. 50:31, 32). The transmission of this document or the revelation of its contents in any manner to any unauthorized person is prohibited." (Irvine, op. cit., pp. 38-39.)

1936. Army Regulations, 330-5.

"For Official Use Only" was dropped from Army Regulations.

The following new definitions were added:

"A document will be classified and marked 'Secret' only when the information it contains is of such nature that its disclosure might endanger the national security, or cause serious injury to the interests or prestige of the Nation, an individual,' or any government activity, or be of great advantage to a foreign nation."

"A document will be classified and marked 'Confidential' when the information it contains is of such a nature that its disclosure, although not endangering the national security, might be prejudicial to the interests or presitge of the Nation, an individual, or any government activity, or be of advantage to a foreign nation."

"A document will be classified and marked 'Restricted' when the information it contains is for official use only or of such a nature that its disclosure should be limited for reasons of administrative privacy, or should be denied to the general public." (Irvine, op. cit., pp. 39-40.)

28 September 1942, OWI Regulation No. 4.

"Secret information is information the disclosure of which might endanger national security, or cause serious injury to the Nation or any government activity thereof."

"Confidential information is information the disclosure of which although not endangering the national security would impair the effectiveness of government activity in the prosecution of war."

"Restricted information is information the disclosure of which should be limited for reasons of administrative privacy, or is information not classified as confidential because the benefits to be gained by a lower classification, such as permitting wider dissemination where necessary to effect the expeditious accomplishment of a particular project, outweigh the value of the additional security obtainable from the higher classification." (Relyea, op. cit., p. 855.)

5 November 1953, E.O. 10501.

E.O. 10501 described classified information as "official information affecting the national defense." Top Secret was defined as "'defense information' requiring the highest degree of protection whose disclosure would cause "exceptionally grave damage to the nation."

Secret information was information whose disclosure would cause "serious damage to the nation." The words "vital" and "important" were used to qualify the examples given of Secret

information. Confidential was defined as information whose unauthorized disclosure "could be prejudicial to the defense interests of the nation." No examples of Confidential were given.

21 June 1957. Legislation Proposed by the Wright Commission.

> "(1) the term 'top secret' or 'atomic top secret' means any information affecting the national defense of the United States in such degree that its unauthorized disclosure could result in exceptionally grave damage to the Nation; and "(2) the term 'secret' or 'atomic secret' means any information affecting the national defense of the United States in such degree that its unauthorized disclosure could result in serious damage to the Nation." (Quoted by Relyea, op. cit., p. 876.)

March 9, 1972. Defense Department Guidelines for Classification.

> "...a determination to classify shall be made only when one or more of the following considerations are present and the unauthorized disclosure of the information could result in a degree of harm to the national security:
>
> 1. The information provides the United States, in comparison with other nations, with a scientific, engineering, technical, operational intelligence, strategic or tactical advantage related to the national defense.
>
> 2. Disclosure of the information would weaken the international position of the United States; create or increase international tensions contrary to U.S. interests; result in a break in diplomatic relations; or lead to hostile economic, political, or military action against the United States or its allies, thereby adversely affecting the national defense.

3. Disclosure of the information would weaken the ability of the United States to wage war or defend itself successfully, limit the effectiveness of the Armed Forces, or make the United States vulnerable to attack.

4. There is sound reason to believe that other nations do not know that the United States has, or is capable of obtaining, certain information or material which is important to the international posture or national defense of the United States vis-a-vis those nations.

5. There is sound reason to believe that the information involved is unique, and is of singular importance or vital to the national defense.

6. The information represents a significant breakthrough in basic research which has an inherent military application potential in a new field or radical change in an existing field.

7. There is sound reason to believe that knowledge of the information would provide a foreign nation with an insight into the war potential or the war or defense plans or posture of the United States; allow a foreign nation to develop, improve or refine a similar item of war potential; provide a foreign nation with a base upon which to develop effective counter-measures; weaken or nullify the effectiveness of a defense or military plan, operation, project, or activity which is vital to the national defense.

The criteria will be reexamined in light of the new Executive order [that is, E.O. 11652]. (Statement of Joseph J. Liebling, Deputy Assistant Secretary of Defense. Senate Hearings on Classification, op. cit., pp. 17409-17410.)

1974. S-2451, a bill introduced by Senator William D. Hathaway.

Secret Defense Data, a single classification defined as information the disclosure of which would adversely affect the ability of the United States to protect itself afainst overt or covert hostile action. (Senate Hearings on Government Secrecy, op. cit., p. 77).

19 February 1976. Definition of Classified Sources and Methods of Information. See footnote 68.

ANNEX B

PRINCIPAL CHANGES EFFECTED BY E.O. 11652

The Order:

- tightens the classification criteria.
- reduces the number of agencies authorized to classify from 47 under E.O. 10501 to 26, only thirteen of which have Top Secret classifying authority.
- establishes schedules for automatic downgrading and declassification of all information except that falling in four exemption categories. (Under E.O. 10501 only one of four groups of information was eligible for downgrading and declassification.) It reduces the downgrading interval from three to two years, and the declassification cycle from 12 years for all levels under the former Order to 10 for Top Secret, eight for Secret, and six for Confidential.
- subjects exempted information to mandatory review for declassification ten calendar years after its origination upon request of a member of the public or of another government agency and to automatic declassification thirty years after its origination unless the head of the originating agency determines

in writing that the exempted information requires additional protection.

- charges the National Security Council with monitoring the implementation of the Order and, to assist the NSC in this function, envisages the creation of an Interagency Classification Review Committee (ICRC). (The ICRC was established by E.O. 11714, dated 24 April 1973, with the following composition: a chairman appointed by the President; representatives of the Departments of State, Defense, and Justice, of the Atomic Energy Commission, the Central Intelligence Agency, and the National Security Council Staff.)
- refers specifically in the preamble to the Freedom of Information Act, stressing that the interests of the United States are best served by making information readily available to the public. In the accompanying statement President Nixon sums up well the dichotomy implicit in FOIA and the classification system: "Clearly the two principles of an informed public and of confidentiality within the Government are irreconcilable in their purest form, and a balance must be struck between them."
- inveighs, in Section 4, against the besetting sins of the classification system throughout its

history--overclassification and unnecessary classification. Offenders "shall be notified" and, in case of repeated abuses, shall be subject to "administrative reprimand." Heads of agencies are to take "prompt and stringent administrative action" against those guilty of unauthorized disclosure.

- provides, in Section 9, a charter for supplementary protection of classified information and material, in particular for codeword compartmentation and the informal compartmentation techniques employed within the Clandestine Service. It reads: "Special Departmental Arrangements. The originating Department or other appropriate authority may impose, in conformity with the provisions of this order, special requirements with respect to access, distribution and protection of classified information and material, including those which presently relate to communications intelligence, intelligence sources and methods and cryptography."

ANNEX C

BREAKDOWN OF THE CLASSIFICATION OF THIS STUDY

OVERALL CLASSIFICATION.....CONFIDENTIAL E2 IMPDET

BY SECTIONS:

INTRODUCTION.....CONFIDENTIAL (Unclassified if asterisked footnote of page 1 is removed.)

PRINCIPAL CONCLUSIONS AND RECOMMENDATIONS.....ADMINISTRATIVE - INTERNAL USE ONLY

DEVELOPMENT OF THE CLASSIFICATION SYSTEM.....UNCLASSIFIED

THE FUNCTIONING OF CLASSIFICATION WITHIN CIA.....CONFIDENTIAL

Misclassification.....CONFIDENTIAL

Related Issues.....Confidential

Reasons for Misclassification.....ADMINISTRATIVE - INTERNAL USE ONLY

Anomalies in the Handling of Top Secret Material.....CONFIDENTIAL

Exemption, Downgrading, and Declassification.....ADMINISTRATIVE - INTERNAL USE ONLY

Impact of Freedom of Information and Privacy Acts.....ADMINISTRATIVE - INTERNAL USE ONLY

Scope of Noncompliance with E.O. 11652.....CONFIDENTIAL

Effect of Classification on the Agency.....CONFIDENTIAL

THE PROBLEM OF DISCLOSURE.....ADMINISTRATIVE - INTERNAL USE ONLY

CONCLUSIONS AND RECOMMENDATIONS.....ADMINISTRATIVE - INTERNAL USE ONLY

FOOTNOTES.....CONFIDENTIAL (Except for footnote 32, which is Confidential, footnotes as a whole are unclassified, Administrative - Internal Use Only

ANNEX A.....UNCLASSIFIED

ANNEX B.....UNCLASSIFIED

ANNEX C.....UNCLASSIFIED