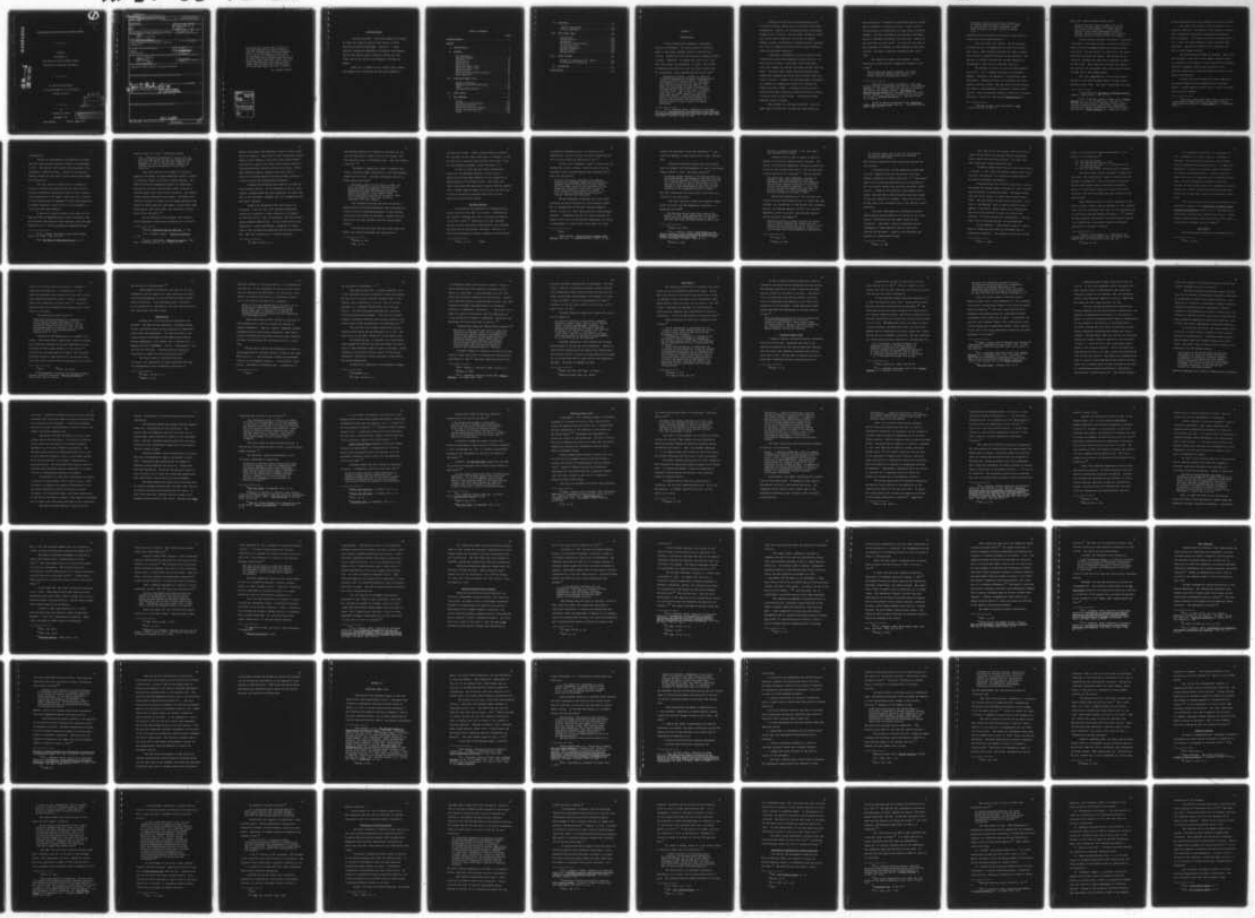
AD-A051 506 AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OHIO F/G 5/4
THE NATIONAL SECURITY CLASSIFICATION SYSTEM.(U)
DEC 77 R L OBORN
UNCLASSIFIED AFIT-CI-78-22 NL

1 OF 3
AD A051 506



# THE NATIONAL SECURITY CLASSIFICATION SYSTEM

A Thesis

Presented to

the Faculty of the Graduate School

University of Missouri-Columbia



In Partial Fulfillment

of the Requirements for the Degree

Master of Arts



by

Richard L. Oborn

December 1977



Dale Spencer Thesis Supervisor

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

**AFIT REPORT DOCUMENTATION PAGE**

READ INSTRUCTIONS BEFORE COMPLETING FORM

| | |
|---|---|
| 1. REPORT NUMBER: CI-78-22 | 2. GOVT ACCESSION NO. |
| 3. RECIPIENT'S CATALOG NUMBER | |
| 4. TITLE (and Subtitle): The National Security Classification System | 5. TYPE OF REPORT & PERIOD COVERED: Master's Thesis |
| 6. PERFORMING ORG. REPORT NUMBER | |
| 7. AUTHOR(s): Captain Richard L. Oborn | 8. CONTRACT OR GRANT NUMBER(s) |
| 9. PERFORMING ORGANIZATION NAME AND ADDRESS: AFIT/CI Student at the University of Missouri, Columbia MO | 10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS |
| 11. CONTROLLING OFFICE NAME AND ADDRESS: AFIT/CI, WPAFB OH 45433 | 12. REPORT DATE: December 1977 |
| | 13. NUMBER OF PAGES: 235 Pages |
| 14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office): 241 p. | 15. SECURITY CLASS. (of this report): Unclassified |
| | 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE |

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public Release; Distribution Unlimited

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

18. SUPPLEMENTARY NOTES

APPROVED FOR PUBLIC RELEASE AFR 190-17.

For James E. Shamlin MSgt USAF
JERRAL F. GUESS, Captain, USAF
Director of Information, AFIT
Deputy Director of Information

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

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

$12.00

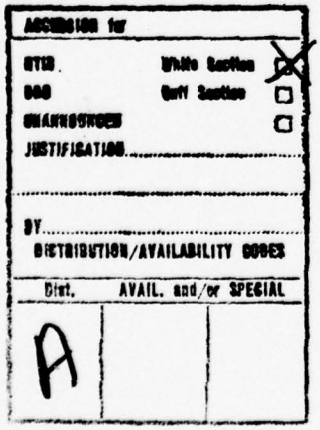
DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

We should keep in mind that it does not take marching armies to end republics. Superior firepower may preserve tyrannies, but it is not necessary to create them. If the people of a democratic nation do not know the basis on which those decisions are being made, then their rights as a free people may gradually slip away, silently stolen when decisions which affect their lives are made under the cover of secrecy.

Sen. Edward Kennedy



## ACKNOWLEDGMENTS

Like most students, I have been shaped and touched by those who sought to pass on some measure of their laboriously acquired knowledge. Thank you. I offer grateful recognition especially to Professor Dale Spencer, who had the onerous task of being my adviser for this study, and to the staff of the Freedom of Information Center.

Above all, I thank my wife, without whose support and empathy this study would not have been completed.

TABLE OF CONTENTS

# CHAPTER I

## INTRODUCTION

A basic dilemma faces democratic government--secrecy or disclosure. The very premise of democracy, power to the people, demands resolution favoring disclosure. Elected officials are given only temporary grants of power. Therefore, the people must know at all times what their proxy, the government, is doing. David Cohen of Common Cause pointed out that the battle becomes one for information. In a Congressional hearing he said:[1]

> Information is power. Secrecy is used with increasing frequency as the means of keeping those in power isolated from the public. The public good depends on its ability to hold government officials accountable for what they do. Yet these officials cannot be held accountable if information about their activities is withheld from the public. Nor is the public inclined to probe when it is kept ignorant of important government matters. Secrecy undermines the public's ability to participate responsibly in the political process, thus threatening, as Madison warned, to make a mockery of popular government.

---

[1] U.S., Congress, House, Committee on Government Operations, Hearings Before a Subcommittee of the Committee on Government Operations on H.R. 4938, H.R. 5983, H.R. 6438, 93rd Cong., 1st Sess., 1973, p. 203.

Insulation of the decision-making process from influences of public debate and criticism has undesirable consequences. Ideally, all information held by government belongs to the citizenry. But the power information wields also can be used to destroy a nation and its people. Complete secrecy could produce a dangerous public ignorance, but a duty of complete disclosure would render impossible effective government operation.

A democratic government strives to preserve basic freedom while maintaining adequate national security. To make secret decisions, a government needs broad public trust that leaders are meeting legitimate national security needs. During the past decade American presidents have hidden their purposes and buried their mistakes under the cloak of secrecy. Vietnam, the Pentagon Papers, Watergate,--all symbols of a dangerously eroded trust between the leaders and their people. A national security culture protected from the influences of American life by a shield of secrecy seems to have evolved. Like absolute power, absolute secrecy corrupts.

The dilemma is by no means one-sided. Since the early days of the nation, the need for some secrecy has

been recognized.[2] Congress has claimed the need to conceal and has operated in executive session. Courts insist on confidentiality of deliberations in jury rooms or judicial chambers. The most confidential proceeding in government may be a conference of Supreme Court justices. Income tax and trade data are kept secret. In practice, the right of the government to withhold is often mandated by the public interest. But here is where the boundaries grow indistinct.

The reasons for secrecy are powerful. Former Secretary of State Dean Rusk emphasized diplomacy is not a *game*.[3]

> Public debate and public diplomacy just cannot resolve the many problems which arise in the normal course of international affairs...

---

[2]The need for secrecy in Congress, courts and business matters is generally discussed in: Louis Henkin, Commentary, "The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers," University of Pennsylvania Law Review 120, (December 1971): 271 at pp. 274-77; "Project -- Government Information and the Right of Citizens," Michigan Law Review 73, (May-June 1975): 971 at 986-88.

[3]Carol M. Barker and Mathew H. Fox, Classified Files: The Yellowing Pages (New York: Twentieth Century Fund, 1972), p. 73.

> Privately, ideas can be tried out tentatively... If negotiations were public, however, it would be very difficult to make adjustments which might influence the public opinion of either side....

President Carter discovered the hazards of open negotiations early in his administration.[4]

There are other real threats. No one seriously disagrees details of weaponry and war plans are validly kept secret. The citizenry does have the right to expect their country's essential secrets will be protected. The concerns of foreign relations and national defense are encompassed in the catch-all "national security."

The trouble is, no one is even sure what national security is. It's a concept concerned with potential dangers. Therefore, the standard is intrinsically vague and elastic. National security is dictated by the chief executive and his policy. The term has no precise meaning but refers to the government's capacity to defend itself against violent overthrow by domestic subversion or external agression. Writing for the journal Foreign Affairs in

---

[4] "Rebuffs at Home, Flak From Abroad," Time, 11 July 1977, pp. 12 and 17.

April 1974, General Maxwell Taylor said:[5]

> National security, once a trumpet call to the nation to man the ramparts and repel invaders, has fallen into disrepute.... It has come to signify in many minds unreasonable military demands, excessive defense budgets and collusive dealings with the military-industrial complex.

Unlike national security, the security classification system is precisely defined, currently by Executive Order 11652 and accompanying National Security Council Directive.[6] Yet few outside, or even inside, the government know much about the system. That system and its evolution, problems and legal basis represent the heart of this study. This study will enlighten the reader to the realities of the system, both as the practice exists on paper and in the workaday world.

The first comprehensive classification system emerged in 1951 when President Harry S. Truman issued Executive Order 10290. This order established the scope

---

[5]Arthur Macy Cox, The Myths of National Security (Boston: Beacon Press, 1975), p. 21.

[6]U.S., President, Executive Order 11652, Federal Register 37, no. 48, 10 March 1972, 5209 and U.S., National Security Council, "National Security Council Directive Governing the Classification, Downgrading, Declassification and Safeguarding of National Security Information," Federal Register 37, 19 May 1972, 10053.

of the system which has since undergone two major revisions.

The system rests upon an inverted pyramid of non-statutory authority. The history of the system's evolution into "hundreds of thousands of stamp-happy bureaucrats" will be detailed. Of primary concern are the provisions of E. O. 11652, the order governing current classification procedures. The order's objectives are desirable; how they are met becomes critical.

The classification system has problems. These will be discussed in relation to their impact upon disclosure of information to the public. This study briefly considers actions of Congress, which early acquiesced to the executive system but of late has bestirred itself to chip away at the monolith.

Finally, the line of executive orders upon which the system depends will be extended soon by President Carter. A draft copy of the new order is being circulated now for public comment.[7]

---

[7]The text of the Carter draft order is printed in "Draft Executive Order Being Circulated Would Revise Classification Procedures," Access Reports 3 (20 September 1977): 1.

# CHAPTER II

# HISTORY

## The Beginning

One particular aspect of governmental secrecy involves withholding information for military reasons. Although the constitutional prerogative of secrecy is limited to "each House" as it applies to the Journal of Proceedings, some degree of secrecy in military and diplomatic affairs has been practiced by the executive branch.[1] A formal classification system to protect certain types of information assumed basic form only 25 years ago, and now has burgeoned into a prevading, bloated system to protect our national security. It all began when the country was yet a colony.[2]

---

[1] U.S., Constitution, art. I, sec. 5.

[2] Most information in this chapter is paraphrased from numerous sources. For more detailed treatment see: Barker and Fox, Classified Files, op. cit.; Cox, The Myths of National Security, op. cit.; James Russell Wiggins, Freedom or Secrecy (New York: Oxford University Press, 1964); Norman Dorsen and Stephen Gillers, ed., None of Your Business: Government Secrecy in America (New York: The Viking Press, 1974); Harold C. Relyea, "The Evolution

Presaging future restrictions, a 1649 Act of Parliament empowered the Secretary of the Army to license all Army news. Information control meant wartime censorship in Colonial days. A 1725 Massachusetts order declared "the printers of the newspapers in Boston be ordered upon their peril not to insert in their prints anything of the public affairs of this province relative to the war without order of the government.[3]

During the Revolutionary War, government secrecy was inconsistent. The 1775 Articles of War prohibited any unauthorized correspondence by soldiers with any enemy and legislation since 1776 forbids spying by civilians in time of war. At times, strict secrecy was imposed. Fortunately, breaches of secrecy were mitigated by slow information

---

of Government Information Security Classification Policy: A Brief Overview (1775-1973)," as printed in U.S., Congress, Senate, Committee on Government Operations, Government Secrecy, Hearings Before a Subcommittee on Intergovernmental Relations on S. 1520, S. 1726, S. 2451, S. 2738, S. 3393, S. 3399, 93rd Cong., 2d Sess., 1974, p. 842; U.S., Congress, House, Committee on Government Operations, Executive Classification of Information--Security Classification Problems Involving Exemption (b) (1) of the Freedom of Information Act (5 USC 552), H. Rept. 93-221, 93rd Cong., 1st Sess., 1973. (Hereinafter, H. Rept. 93-221.)

[3]Wiggins, Freedom or Secrecy, p. 94.

dissemination.

Concern for governmental confidentiality surfaced when the Constitutional Convention opened in Philadelphia in 1787. The adopted rules allowed the proceedings to be conducted in complete secrecy. Records of the meetings remained sealed for more than 30 years before being opened for publication.[4]

The first executive restriction of information related to defense and foreign policy and came in 1790. President Washington asserted the right to limit information dissemination to the public under Article II, section 2 of the Constitution as Commander in Chief when presenting for Senate approval a secret article to be included in a treaty with the Creek Indians.[5]

An executive claim of secrecy first arose in 1792 when the House of Representatives sought information from the President concerning an Indian massacre along the upper Wabash River of a military expedition commanded by Major

---

[4]U.S. v. Nixon, President of the United States, 418 US 683 (1974), note at p. 20.

[5]Cox, The Myths of National Security, p. 33.

General Arthur St. Clair.[6] The House resolved

> that a committee be appointed to inquire into the causes of the failure of the late expedition under Maj. Gen. St. Clair, and that said committee be empowered to call for such persons, papers, and records, as may be necessary to assist their inquiries.[7]

Since this was the first demand for executive papers by the House, President Washington wished it should be conducted rightly and called a Cabinet meeting. The House received the appropriate papers, but Washington asserted an executive discretionary power to refuse to disclose papers that would injure the public. The Cabinet reached several procedural conclusions: the House could *institute queries; it might call for papers generally;* the Executive should hand over such papers "as the public good would permit" and refuse those "the disclosure of which would injure the public."[8]

By its handling of this episode, the executive branch expressed a theoretical foundation for a claim to

---

[6]Relyea, Government Secrecy Hearings, p. 844.

[7]U.S., Congress, House, 3 Annals of Congress, p. 493.

[8]Clark R. Mollenhoff, Washington Cover-up (New York: Doubleday and Co., Inc., 1962), p. 213.

secrecy and advanced the President's power to refuse information to Congress. This claim to deny information evolved along a narrow channel to executive orders establishing a classification system, and along a much broader channel to wide-ranging modern claims of executive privilege. While some scholars disagree, Congress holds the issue of executive privilege separate from the narrower concerns of a classification and declassification system.[9]

Congress has recognized the propriety and need for some executive secrecy. At the beginning of the St. Clair inquiry, Congress asked the State Department to report only what in the President's judgment was "not incompatible with the public interest."

Despite the recognition that some secrecy was necessary, it was not until 1796 President Washington asserted his authority to deny information to Congress. As with the 1792 St. Clair investigation, the 1796 investigation prompted high emotion. In 1794, Chief Justice Jay negotiated a treaty with England, attempting to resolve some of the controversies remaining from the Revolutionary War. When Jay returned with "a treaty containing

---

[9]H. Rept. 93-221, p. 2.

extraordinary benefits for Federalist interests and not one item favorable to anyone south of the Potomac, the rage against it was, as Washington said, 'like that against a mad dog.'"[10]

Obligated to appropriate funds to implement the treaty, the House sought instructions to Jay and documents supporting the treaty. President Washington refused the House request and said:[11]

> ...the papers called for can throw no light, and as it is essential to the due administration of government that the boundaries fixed by the Constitution between the different departments should be preserved, a just regard to the Constitution and to the duty of my office, under all circumstances of this case, forbids a compliance with your request.

The President discussed the need for secrecy in negotiations with foreign governments and cited Constitutional vesting of treaty-making powers in the President with advice and consent of the Senate. Nowhere does the Constitution include the House into the treaty-making process.

Not only did the furor over the treaty shock the House, the earliest precedent for leaking secret

---

[10] Relyea, p. 845.

[11] Cox, p. 33.

information occurred. Senator Stevens Mason of Virginia was incensed, as were other Southerners in Congress, at the way the secret treaty had been handled and he sent a copy to a Philadelphia newspaper, which published it.[12]

In the St. Clair and Jay treaty Congressional inquiries, the president asserted a broad claim of executive privilege based generally on the separation of powers doctrine of the Constitution. This study will later explain how the separation of powers doctrine combines with a claimed inherent power of secrecy for the executive to form an executively espoused legal basis for the executive classification system.

## National Defense

No directives for protection of information were issued until the Civil War, but "Secret," "Confidential," and "Private" markings were used on military information in the War of 1812.[13] During the Civil War President Lincoln strictly controlled communications--the telegraph, the mails and to some extent, the press. Secretary of State William Seward maintained a network of secret agents

---

[12] Ibid., p. 34.

[13] Ibid.

to apprehend Confederate spies, collaborators and sympathizers, and the military controlled communications and civilians within the shifting war zone.[14]

Various Union commanders sought to censor news dispatches and accredit newsmen. Near the end of the war, President Lincoln advised General John Schofield how to deal with the press:[15]

> You will only arrest individuals and suppress assemblies or newspapers when they may be working palpable injury to the military in your charge, and in no other case will you interfere with the expression of opinion in any form or allow it to be interfered with violently by others. In this you have a discretion to exercise great caution, calmness and forbearance.

The War Department established the first formal peacetime security procedures by issuing General Orders No. 35, Headquarters of the Army, Adjutant General's Office, on April 13, 1869, which protected fixed seacoast defenses: "Commanding officers of troops occupying the regular forts built by the Engineer Department will permit no photographic or other views of the same to be taken

---

[14] Ibid.

[15] James Randall, Constitutional Problems Under Lincoln (New York: D. Appleton and Co., 1926), p. 508.

without the permission of the War Department."[16] The order was repeated in Army regulations of 1881, 1889 and 1895.

Relations with Spain deteriorated and possible open war prompted the War Department to issue a new General Order on March 1, 1897. The order directed:[17]

> No persons except officers of the Army and Navy of the United States, and persons in the service of the United States employed in direct connection with the use, construction or care of these works, will be allowed to visit any portion of the lake and coast defenses of the United States without the written authority of the Commanding Officer in charge.

The order prohibited also any written or pictorial description of the facilities.

The order received a slight but important change before inclusion into War Department regulations. A paragraph indicated[18]

> ...the Secretary of War would grant special permission to visit these defenses only to the United States Senators and Representatives in Congress who were officially concerned therewith and to the

---

[16] Relyea, pp. 846-7.

[17] U.S., Congress, Senate, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Book VI, S. Rept. 94-755, 94th Cong., 2d Sess., 1976, p. 315.

[18] Relyes, p. 847.

> Governor or Adjutant General of the state where such defenses were located.

Congress acted in 1898 to impose an explicit penalty for willfully exposing coastal defenses. The statute sanctioned War Department information protection directives and increased the order's force by providing criminal penalties for violations.[19] The law provided

> any person who...shall knowingly, willfully or wantonly violate any regulation of the War Department that has been made for the protection of such mine, torpedo, fortification or harbor-defense system shall be punished, ... by a fine of not less than one hundred nor more than five thousand dollars, or with imprisonment for a term not exceeding five years, or both.

Though Army regulations of 1901 continued provisions limiting Congressional access to coastal and lake defenses, new regulations in 1908 omitted such references. Instead, the language admitted for the first time War Department efforts to protect fixed defenses against foreign military intelligence.[20]

> Commanding officers of posts at which are located lake or coastal defenses are charged with the responsibility of preventing, as far as practicable, visitors from obtaining information relative to such defenses which would probably be communicated

---

[19] 30 Stat. 717.

[20] Relyea, p. 847.

> to a foreign power, and to this end may prescribe and enforce appropriate regulations governing visitors to their posts.

That provision appeared in Army regulations through the 1917 edition.

In February 1912, the War Department established its first complete system for protection of national defense information in General Orders No. 3.[21] The general order did not prescribe particular security markings but did list certain records that would be considered "confidential": submarine mine projects; land defense plans; tables, maps and charts showing defense locations; number of guns and character of armament. These records were to be kept under lock "accessible only to the officer to whom entrusted."

The order established an accountability system which required serial numbers to be issued for all "confidential" information with the number marked on the document(s). Each year, officers responsible for the safekeeping of these materials were to check their location and existence. Access to such documents was granted all commissioned officers.

---

[21] Ibid., p. 848.

Until the turn of the century, policy directives explicitly protected only national defense information about coastal and lake fortifications. But other documents apparently enjoyed protection also.

Brigadier General Arthur Murray, Chief of Artillery, on October 3, 1907, wrote the Adjutant General about use of the word "confidential" as a marking on communications.[22] No directive defined "confidential."

Murray believed the situation ridiculous, citing as an example one message marked "confidential" that contained merely formulas for making whitewash. The general posed questions which continue to haunt classification users today. How long should information be classified? If an item is "confidential" does it remain classified once it appears in the press? Harbor charts are "confidential" yet can be found attached to walls of civilian fire stations. If certain manuals are "confidential," why are they issued to enlisted men and civilian employees?

Murray lamented: "Some officers keep all "confidential' communications locked up and others take no precautions whatsoever." He proposed a time limit on the

---

[22] Ibid., p. 849.

effect of the marking and urged establishment of four degrees of confidentiality:[23]

(1) For your eyes only;
(2) For commissioned officers only;
(3) For official use only, i.e., available to all military personnel;
(4) Not for publication (outside military channels).

The Chief Signal Officer attempted to explain the situation. The "confidential" manual in question was not actually "confidential," only "restricted distribution." But the Chief Signal Officer understood the problem, agreed a classification system was a step in the right direction, and noted the matter had been referred to the General Staff.

Major General William P. Duvall, Assistant to the Chief of Staff, issued a memo on November 12, 1907, stating "that the idea of setting time limits on the confidentiality of particular items was hardly practicable...."[24] However, the memo admitted "confidential" was overused and directed it be employed more judiciously, based on considered appraisal of a document's contents.

---

[23]Daniel J. Birmingham, Jr., "Problems in the Security Classification System" (Air War College paper, Maxwell AFB: Air University, 1975), pp. 4-5.

[24]Relyea, p. 849.

War Department Circular No. 78 of November 21, 1907, encompassed the correct usage of "confidential" markings. The circular dealt primarily with internal military communications and publications. It marked the beginning of a policy of protecting internal documents for reasons of national defense. Further, protective labels used had to be explained by an accompanying statement. Use of an explanatory statement maintained a rational and self-evident policy for safeguarding internal information. Future classification would be explicitly defined but in many cases usage would obliterate rationality.

The circular's provisions were not included in Army regulations, except in the Compilation of General Orders, Circulars and Bulletins issued in 1916. The anonymity of Circular No. 78 along with confusion over use of a "confidential" marking implies the directive had little impact in curtailing the improper use of the label.[25]

## World War I

The United States declared war on Germany April 6,

---

[25] Ibid., p. 850.

1917. The action prompted new regulations to protect national defense information. The American military began working with its British and French allies and had an opportunity to observe security systems in other armies. Development of a codified system of information classification was prompted by the need to protect allied information. Translations of British and French training documents with classification markings were transmitted to the U.S. to aid in training. Also, the rapid officer force expansion made it impossible to rely on circumspection in security matters, as expected of professionals.

General Headquarters of the American Expeditionary Forces published General Orders No. 64 on November 21, 1917, establishing the classifications of Confidential, Secret and For Official Circulation Only.[26]

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

---

[26] Ibid., p. 851.

> Secret in the most complete understanding of that term. There are no degrees of secrecy in the handling of documents so marked.
>
> * * * * * * * *
>
> Orders, pamphlets of instructions, 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.

One must wonder about the propriety of any administrative marking for information that "would result in no harm to the Allied cause." The concept of national harm became the overriding concern in subsequent classification definitions. As the basis for classifications, the concept of harm would become both the definitional Maginot Line and the classification system's Achilles' heel. If information is harmful to the nation it must remain undisclosed, but who decides the harm's magnitude, and how?

The system was patterned after British and French procedures. The order provided limitations on reproduction and distribution. Also, the order acknowledged prior usage of the markings Confidential and Secret and admonished previous indiscriminate use of the terms.

The War Department was quick to authorize use of the protective labels throughout its jurisdiction. The three

terms received more precise definition in "Changes in Compilation of Orders No. 6" of December 14, 1917. Materials designated Secret would be hidden from view but those labeled Confidential might circulate "to persons known to be authorized to receive them."[27] The third marking restricted information from communication to the public or the press.

Additionally the order states:[28]

> Publishing official documents or information, or using them for personal controversy, or for private purpose without due authority, will be treated as a breach of official trust, and may be punished under the Articles of War, or under Section I, Title 1, of the Espionage Act approved June 15, 1917.

Reference to the Espionage Act is somewhat confusing. The statute didn't specifically sanction information protection practices of the War Department nor were the orders written under authority of the statute.[29] Invocation of the Espionage Act probably "was considered advisable because so many officers of the war-time Army were drawn from civilian life and therefore would not have

---

[27] Ibid.

[28] Ibid., pp. 851-2.

[29] "Developments in the Law--the National Security Interest and Civil Liberties," Harvard Law Review 85 (April 1972):1197 at 1232-41.

the instincts of professionals."[30]

Establishment of protective markings for official information did not begin out of legal necessity for administering the Espionage Act but were merely copied from the French and British. Given widespread public acceptance of the importance of censorship at the time, the directive's weak legal basis was never tested.

## Between Wars

Between wars, little classified information was produced. The Navy and War Departments developed systems to hold information about military planning and operations within their own departments. The Army continued to use classifications established by the Expeditionary Forces. The War Department's first change came in January 1921. A pamphlet entitled "DOCUMENTS: 'Secret,' 'Confidential,' and 'For Official Use Only'," compiled wartime information regulations to remain in force during peacetime.[31]

The three levels of classification were: (1) Secret--for information "of great importance and when the safeguarding of that information from actual or

---

[30] H. Rept. 93-221, p. 4.

[31] Relyea, p. 853.

potential enemies is of prime necessity;" (2) Confidential--for material "of less importance and of less secret nature than one requiring the mark Secret, but which must, nevertheless, be guarded from hostile or indiscreet persons;" and (3) For Official Use Only--for 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.[32]

These regulations neither related to provisions of the Espionage Act of 1917 nor limited the markings to defense information. They did, however, emphasize personal responsibility for restricting information. Each classification included the classifying officer's name, authority and date, and provisions for declassification at a later time.

Definitions of Secret and Confidential as found in Navy Regulations of 1932 were similar to those in use today. Words such as "... the disclosure of which would be highly inimical to the national interest..." define Secret information. Confidential information was "...prejudicial to

---

[32]Ibid.

the interests of government...."[33]

The Army may have felt it missed something, so in a 1935 regulation revision introduced a Restricted marking. The mark was to be used to protect research work on the "design, test, production, or use of a unit of military equipment or a component thereof which was to be kept secret." The Army threatened Espionage Acts sanctions by marking restricted documents: "Notice--this document contains information affecting the national defense of the United States within the meaning of the Espionage Act."[34]

This was the first linkage between the security classification system and the Espionage Act of 1917. The actual lack of any legal linkage will be discussed later.

The following year, in February 1936, Army regulations dropped For Official Use Only and brought the definitions of other markings closer to those of the Navy. Secret information could cause "serious injury" to the nation; information "prejudicial to the interests" of the nation was marked Confidential.

Of particular importance is the broadened category

---

[33]Birmingham, p. 8.

[34]H. Rept. 93-221, p. 5.

of information which classifications covered. Foreign policy material and "the interests or prestige of the Nation, an individual, or any government activity" fell within the protective umbrella of classification. According to National Archives historian Dallas Irvine, this 1936 regulation extended "the applicability of protective markings to 'nondefense' information.... The effect was to apply the menace of prosecution under the Espionage Act to the protection of whatever 'nondefense' information War Department officials might want to protect."[35]

Congressional researcher Harold Relyea summarizes:[36]

> The point is that by the late 1930's, restriction labels knew no bounds: they could be applied to virtually any type of defense or nondefense information; they pertained to situations involving "national security," a policy sphere open to definition within many quarters of government and by various authorities; and they carried sanctions which left few with any desire to question their appropriateness or intention.

President Franklin D. Roosevelt initiated the first executive order (E.O. 8381) in the security classification field March 22, 1940.[37] Entitled "Defining Certain Vital

---

[35] See: Relyea, p. 854 and H. Rept. 93-221, p. 6.

[36] Relyea, p. 854.

[37] U.S., President, Executive Order 8381, Federal Register 5, 26 March 1940, 1145.

Military and Naval Installations and Equipment," the order cited a 1938 law as authority to protect against information dissemination about specified sensitive military and naval installations and equipment, and to make it a crime to make any photo, sketch or representation of them.[38] Violators of the law could receive a $1,000 fine, up to a year in jail, or both.

President Roosevelt expansively ordered the use of control labels on

> all official military or naval books, pamphlets, documents, reports, maps, charts, plans, designs, models, drawings, photographs, contracts, or specifications which are now marked under the authority of the Secretary of War or the Secretary of the Navy as 'secret,' 'confidential,' or 'restricted,' and all such articles or equipment which may hereafter be so marked with the approval or at the direction of the President.[39]

President Roosevelt's order adopted the markings and rationale of the War and Navy Departments. Control of classification modification and application remained with the military with no civilian oversight explicitly provided. Use of the markings only by armed services was apparently presumed. World War II changed all that.

---

[38] Public Law 418, 75th Cong., 52 Stat. 3.

[39] Executive Order 8381, pp. 1147-8.

## World War II

The outbreak of World War II dictated a more widespread use of an information protection system. Government-wide security classification procedures were issued in September 1942 by the Office of War Information (OWI). Established by Executive Order 9182 on June 13, 1942, OWI issued a regulation on September 28 controlling the identification, handling and dissemination of sensitive information. It also warned against overclassification.[40]

Three categories of classified information were defined.[41]

> 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 governmental activity in the prosecution of the 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.

---

[40] Relyea, p. 855.

[41] H. Rept. 93-221, pp. 7-8.

In 1943 a Security Advisory Board was formed to coordinate and advise on all information security matters. The National Security Act of 1947 created the National Security Council as the Board's successor. The Council was to consider and study security matters involving executive departments and agencies, and to make recommendations to the President. Former Ambassador Robert Murphy described the mushrooming of national security secrecy.[42]

> There had been practically no security precautions in the State Department prior to the war. Suddenly we had too much. Every report seemed to contain secrets; the most innocuous information was 'classified;' a swollen staff of security agents hampered the work of everybody.

## Executive Order 10290

A powerful emotion controlled post-war information security actions--fear. Americans were awed by the destructive potential of the atom and many were obsessed with the belief that communist influence would destroy their way of life. The war habit of secrecy was hard to break when confronted with this newly perceived evil.

---

[42]Barker, p. 12.

Congressional concern was translated into the Atomic Energy Act of 1946.[43] The Act, amended in 1954, created the first and only statutory classification system; this one just for atomic information.

In 1950 President Truman superseded Roosevelt's E. O. 8381 with Executive Order 10104, "Definitions of Vital Military and Naval Installations and Equipment."[44] The order kept the earlier three categories of classification and formally added Top Secret, previously incorporated into military regulations to coincide with classification levels of our allies. Throughout the historical usage of classification markings, including this order, the directives applied only to protection of military secrets and, rarely, foreign policy or diplomatic relations. The only exception was communications secrecy protected by the Espionage Act.

> ...It is necessary, in order to protect the national security of the United States, to establish a system for the safeguarding of official information the unauthorized disclosure of which would or could harm, tend to impair, or otherwise threaten the security of the nation. ...It is desirable and proper that minimum

---

[43] Atomic Energy Act, Public Law 83-703.

[44] U.S., President, Executive Order 10104, Federal Register 15, 1 February 1950, 597.

> standards for procedures designed to protect the national security against such unauthorized disclosure be uniformly applicable to all departments and agencies of the executive branch of the government and be known to and understood by those who deal with the Federal Government....[45]

With this stated purpose, President Truman's Executive Order 10290, issued September 24, 1951, extended the security classification system to all executive departments and agencies.[46] The order constituted the first permanent consolidated system for safeguarding defense information during either war or peace. Illustrating the need for such a system, Truman cited a confidential study by Yale University of censorship breaches, which reported 95 per cent of all secret government information was being published in the press.[47]

---

[45] 3 CFR, 1 January 1949-31 December 1953 Compilation (Washington: Government Printing Office, 1958), p. 789. All quotations from this executive order can be found in this section.

[46] U.S., President, Executive Order 10290, Federal Register 16, 27 September 1951, 9795. The order's provisions are paraphrased to provide easier reading. Those willing to tackle the governmental jargon should refer to the complete text in the Federal Register.

[47] New York Times, 5 October 1951, p. 12.

Perhaps President Truman reached the wrong conclusion. If that much supposedly secret information had been literally given to the enemy and the country had suffered no breach in its defenses, then the information couldn't have been that important initially. Maybe what was needed was less classification, not more.

Entitled "Prescribing Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States," the order retained the four-tiered classification system without adequately differentiating between the various markings. The Top Secret label was required on information needing the highest degree of protection, the disclosure of which "... would or could cause exceptionally grave danger to the national security." While this definition approximates the one in use today, Secret and Confidential were defined more vaguely. The authors were apparently not aware or chose to ignore the definitions used by the Navy. Secret was a category which included information requiring an "extraordinary degree of protection;" Confidential required only "careful protection." The fourth category,

Restricted, applied to information requiring "protection against unauthorized use or disclosure."

The order cautioned the markings should "be used only for the purpose of identifying information which must be safeguarded to protect the national security." But there was no limitation on the number of people allowed to designate classified security information--"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." Nor did the order define "appropriate classifying authority."

As with prior directives, the order wrapped itself in an aura of legal authority though it cited no constitutional or statutory basis. President Truman relied on implied powers under the "faithful execution of laws" clause. The order could not bind private citizens to its observance, but the Preamble stated:

> All citizens of the United States who may have knowledge of or access to classified security information are requested to observe standards established in such regulations with respect to such information and to join with the Federal Government in a concerted and continuing effort to prevent disclosure...to persons who are inimical to...the United States.

Executive employees were subject to administrative penalties,

including loss of their jobs. Violation of the order was not a criminal offense.

Operating regulations for safeguarding defense information were part of the executive order.[48] They were divided into seven parts: general provisions, definitions, responsibilities, classification rules, dissemination, handling and interpretation.

The "General Provisions" discussed the purpose and scope, and enumerated the four categories of classification. The order had no effect on any statutory standards, such as those controlling atomic energy material. Only official U.S. government information and that received from foreign governments was protected.

The "Definitions" section was awash with governmental jargon and vague, imprecise definitions. An "appropriate classifying authority" was anyone authorized to classify, declassify, upgrade (assign a higher classification) or downgrade (assign a lower classification) information. With unlimited delegation power by agency heads, authority devolved to virtually anyone within the executive branch.

---

[48] See: John A. Gangloff, "Safeguarding Defense Information," (M.A. Thesis, University of Missouri-Columbia, 1971), pp. 69-71.

The third section, "Responsibilities," informed executive employees of their responsibility to protect classified information and urged all to be familiar with the order's provisions. While an agency head could delegate classification authority, officials were asked not to abuse this power. Each agency head was empowered to issue his own additional rules, thus controlling, as he saw fit, information originating within that particular organization.

"Classification Rules" covered general and special classification procedures plus instructions for upgrading, downgrading and declassification. No markings but the four classification categories were allowed, and then only for information protected in the interests of national defense. Like the definitions, the type of information contained in any category was vaguely defined and open to judgment. Each department head was charged with interpreting those definitions and making the judgment.

The special classification rules detailed procedures for handling some special types of information and additionally restricted classification authorities. A classification change must receive the consent of the appropriate classifying authority, usually the original

classifier. Classified information received from a foreign government was to be given equal or greater protection than that required by the originator. A multi-part document received an overall classification at least as high as the highest classified component part.

Upgrading classified information could be accomplished only by the originator. No automatic declassification system was required but an optional automatic procedure was to be used "whenever practicable." The optional system called for classifying officials to note on the classified material a date or event whose passage would free the material for automatic downgrading or declassification. The order specified constant review to determine when documents could be downgraded or declassified but no implementing procedure was adopted.

Dissemination of classified information was limited to executive branch members with a "need to know." Only the head of an agency could approve dissemination of his classified information outside the executive branch. Similarly, the originating agency controlled reproduction of Top Secret and Secret documents. Even members of Congress had to comply with conditions prescribed by the classifiers.

The order contained specific instructions for

marking, transmitting, storing and destroying classified information.

The Attorney General was assigned overall responsibility for interpretation of the regulations. His effectiveness was hampered since he could only give an opinion upon request and had no authority over department heads. Besides, President Truman promised his own press relations office would handle complaints of overclassification or abuse of power.

President Truman's order suffered heavy criticism. The order did anything but open up government to public view. Professional news organizations and members of Congress quickly denounced the directive. Truman must have been bewildered. He did not see the order aimed at press or public but at spies who already had demonstrated they could obtain vital secrets from the government.

The press charged the system would allow officials to cover-up mistakes and political intrigues under the veil of national security while allowing official leaks. In later times and under different executive orders, this prognostication proved all too correct. The New York Times

summarized the criticism in an editorial:[49]

> The Presidential order is broad in its powers but vague in its definitions. A striking weakness is the failure to make any provision for systematic and periodic review of how it is being put into use. Vast discretion is placed in the hands of a large number of officials with no adequate check upon how that discretion is exercised. The result is that the effect of this order will depend on a considerable amount of very fallible human judgments.

The order failed to curb overclassification, to provide any review authority and to allow a classification appeal procedure.[50]

The President, reacting righteously to such criticism, reaffirmed his belief that

> protection of military secrets should not be made a cloak of secrecy or cover for withholding from the public information about their government which should be made known to them...information shall not be classified and withheld from the public on the ground that it affects national security, unless it is in fact necessary to protect such information in the interests of national security.[51]

---

[49] New York Times, 28 September 1951, p. 30.

[50] Benedict K. Zobrist II, "Reform in the Classification and Declassification of National Security Information: Nixon Executive Order 11652," Iowa Law Review 59 (October 1973): 110 at 118.

[51] "When Mr. Truman Sounded Off on Responsibilities of the Press," Editor and Publisher, 13 October 1951, p. 62.

At its October 1951 meeting, the Associated Press Managing Editors Association unanimously passed a resolution condemning the new order and saying it was "...issued without any showing of necessity."[52] President Truman disagreed, saying he had "...issued this order with great reluctance, and only when...convinced after lengthy consideration that it was necessary to protect the United States...."[53]

Editor and Publisher expressed belief that Truman had been too heavy-handed: "Information of a security nature can be protected without the creation of 60-odd government censorship offices which can ring Washington with an iron hand."[54]

President Truman must have forseen the potential for abuse. A memorandum issued with the order said:[55]

> To put the matter bluntly, these regulations are designed to keep security information from potential enemies and must not be used to withhold nonsecurity information or to cover up mistakes made by any official or employee of the Government.

---

[52] Editor and Publisher, 6 October 1951, p. 12.

[53] Editor and Publisher, 13 October 1951, p. 7.

[54] Ibid., p. 62.

[55] Washington Post, 26 September 1951, p. 3.

Senator Blair Moody of Michigan summarized Congressional criticism of the order.[56]

> ...Two things must be done in this field. The first one is to protect the United States against the release of information which would be of value to an enemy or potential enemy.
>
> The second is to protect the public of the United States against having the public's business kept secret when there is no real reason why it should not be made public.

An abortive attempt was made to overturn the directive when Senator John W. Bricker (R-Ohio) introduced S. 2190 on September 28, 1951, to "prohibit unreasonable suppression of information by the Executive Branch of Government."[57]

Actually, the New York Times agreed with the need for secrecy but disagreed with the particular vehicle of application.[58]

> It goes without saying that there are some matters essential to the national defense that need to be kept secret. It is also apparent that we would profit by some uniform system of classification and release. But after those things are taken into account there is still reason to question the wisdom of the form in which action has been taken.

---

[56] U.S. Congress, Senate, 82d Cong., 1st Sess., 1951, Congressional Record 97:12508.

[57] Barker, pp. 12-13.

[58] New York Times, 28 September 1951, p. 30.

## Executive Order 10501

On November 6, 1953, President Dwight D. Eisenhower responded to continued criticism of the classification system and announced Executive Order 10501, "Safeguarding Official Information in the Interests of the Defense of the United States."[59] Eisenhower had campaigned on a promise to conduct an open government. But once in office, faced with pressures for secrecy, he made some significant changes yet continued the information security system begun by President Truman.

Despite Joseph Stalin's death in March 1953, the Cold War did not disappear and the arms race became a strong justification for safeguarding official information.[60] Joseph R. McCarthy pursued his overzealous investigations; the Middle East was a potential problem area; and China, backed by the U.S.S.R., emerged as a potential United States enemy.

The order was designed to eliminate some potential

---

[59] 3 CFR, 1 January 1949-31 December 1953 Compilation (Washington: Government Printing Office, 1958), pp. 979-804. Executive Order 10501, Federal Register 18, 9 November 1953, 7049. Provisions of this order are paraphrased.

[60] Cox, p. 48.

for abuse which existed under its predecessor. The White House said:[61]

> throughout the lengthy consideration of this order it has been the purpose to attain in it the proper balance between the need to protect information important to the defense of the United States and the need for citizens of this democracy to know what their government is doing.

The order's stated purpose was to preserve national security by insuring "that certain official information affecting national defense be protected uniformly against unauthorized disclosure." Also, the Preamble emphasized "... it is essential that the citizens of the United States be informed concerning the activities of their government."

The order limited classification to three categories, and eliminated the Restricted category allowed in the Truman order. It reduced the number of agencies authorized to originate classifications and defined a more elaborate system of declassification.

In keeping three of the four classification categories, the new order redefined Top Secret, Secret and Confidential. A slightly improved definition for Top Secret was written.

---

[61] Wiggins, p. 102.

> Top Secret: ...shall be authorized...only for defense information or material which requires the highest degree of protection. It shall be applied only to that information or material... the unauthorized disclosure of which could result in exceptionally grave damage to the nation such as leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.

The Secret definition similarly provided examples of material to be protected.

> Secret: ...shall be authorized...only for defense information or material the unauthorized disclosure of which could result in serious damage to the nation, such as by jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important intelligence operations.

Unfortunately, the lowest classification's application was least definitive. No examples of the types of information certified by the marking were given. The judgmental factor seems to play a larger part in the Confidential definition than it plays in the two higher classifications.

> Confidential: ...shall be authorized...only for the defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.

Order 10501 limited classification authority. Not all executive agencies had the power to classify. Presidential delegation was necessary, and the delegation was based upon an agency's responsibility for national defense matters. Executive agencies were divided into three groups. One group had no authority to classify; a November 5, 1953, memo specified 28 agencies without such power. Another group (17) had limited authority; only the head of the department or agency could classify. The third group received full classification powers and could delegate the authority to classify to "responsible officers or employees." Nonetheless, delegation had to be limited "as securely as is consistent with the orderly and expeditious transaction of Governmental business."

The Foreign Operations and Government Information subcommittee found controls on the delegation of the classification power did not work very well. An August 1971 questionnaire sent to executive agencies discovered 55,000 persons authorized to classify.[62] Apparently

---

[62] Part 7, pp. 2929-37.

proliferating the delegated power to classify, an Army regulation permitted information to "...be classified Confidential by, or by authority of, any commissioned or warrant officer or responsible civilian officer."[63] That's not a very restricted authority. A former high official in the Air Force Department estimated in 1956 that as many as a million people were classifying documents.[64]

The order held authorized classifiers responsible for the propriety of classifications and agency heads were called upon to conduct a continuing review of classified material, hoping some information would be downgraded or declassified. Formal procedures were to be established. Once classified information "no longer required its present level of protection in the defense interest....," it was to be classified. The classifying official was to indicate the time or condition when a document could be declassified

---

[63] U.S., Congress, Senate, Committee on Government Operations and Committee on the Judiciary, Executive Privilege, Secrecy in Government, Freedom of Information, Hearings Before the Subcommittee on Intergovernmental Relations on S. 858, Con. Res. 30, S.J. Res. 72, S. 1106, S. 1142, S. 1520, S. 1923, and S. 2073, Vol. III, 93rd Cong., 1st Sess., 1973, pp. 600-1.

[64] Ibid., p. 601.

without a formal review.

Automatic declassification would be used "to the fullest extent," but it still remained nonmandatory. Another department could request downgrading or declassification of a document in its possession, to which the originator must agree. The Department of Defense was first to install an automatic declassification system in 1960.[65] Classified information would be downgraded at three-year intervals and declassified at the end of 12 years. The only problem was that most sensitive subjects and information were exempted from declassification. The order's attempts to accelerate the declassification process proved ineffective.[66]

Order 10501 purposely emphasized security rather than access to material. It dealt extensively with the details of protecting classified information. Sections five through nine elaborated on the mechanics of classification marking, specified storage and custodial procedures; delineated rules for dissemination, described rules for transmitting classified material, and told

---

[65] Relyea, p. 864.

[66] Zobrist II, p. 121.

agencies how to destroy classified records. The main concern was for the safeguarding of information.

Several sections of the order promoted reviews of classified information. Most review procedures were directed toward safeguarding information but Section 18 did recognize the need "...to insure that no information is withheld hereunder which the people of the United States have a right to know...." As with previous orders, the Attorney General was entrusted with interpretation of the regulations, but only upon receipt of a request by the head of a department or agency.

One last critical concern about E.O. 10501 was the lack of sanctions against both those who improperly disclosed classified information and those who over-cautiously classified information. Section 19 specifies:

> The head of each department and agency is directed to take prompt and stringent administrative action against any officer or employee of the United States, at any level of employment, determined to have been knowingly responsible for any release or disclosure of classified defense information or material...and where a violation of criminal statutes may be involved, to refer promptly to the Department of Justice any such case.

Thus, it seems the order did not specifically invoke the threat of the Espionage Act against those who improperly disclosed classified information. And Section

19 did not call for sanctions against those who wrongly overclassified information.

Executive Order 10501 corrected many of the recognized faults of its predecessor as Editor and Publisher magazine recognized when it commented:[67]

> President Eisenhower and Attorney General Brownwell are to be complimented on the new Executive Order on safeguarding defense information. It is a vast improvement over the order former President Truman invoked in September 1951 and is recognized as such by most newsmen.

But the magazine warned of the always present temptation for officials to hide information from prying newsmen. The Associated Press Managing Editors Association expressed "a grateful but guarded approval...."[68]

In 1956, James Russell Wiggins zeroed in on a less than perfect portion of the order when he wrote:[69]

> Far less objectionable than the order which preceded it, the new executive order still is open to some criticism. The most serious of these is its failure to provide for an adequate weighing of the needs of security and information at the time of classification....

---

[67] "Security Order," Editor and Publisher, 14 November 1953, p. 44.

[68] Ibid., p. 11.

[69] Wiggins, p. 102.

In other words, the indiscriminate use of the "security" veil continued to feed the persistent bugaboo of over-classification.

The Eisenhower order did little to open information to scientists since it continued the "need-to-know" criteria for access to classified information. This meant a person must be granted a security clearance before being allowed access to classified material. Natural scientific curiosity was not sufficient to pass the bureaucratic need-to-know barrier. Scholars had similar problems in gaining access to classified government records.[70]

## Modifications

Criticism and organizational change prompted numerous clarifying directives and new orders.

On November 5, 1953, President Eisenhower issued a memo to accompany E.O. 10501. It named 28 agencies which were without original classification authority. Limited authority was granted 17 agencies.[71] Six years later, on

---

[70] Barker, p. 13.

[71] 3 CFR, 1 January 1959-31 December 1963 Compilation (Washington: Government Printing Office, 1964), p. 803.

May 7, 1959, the President updated the list of agencies without original classification authority by adding two.[72]

The death of President Eisenhower's secretary of state, John Foster Dulles, prompted Executive Order 10816.[73] The order opened access to classified documents to historical researchers. The historian had to be "trustworthy" and the research had to be "clearly consistent with the interests of national defense." Primary White House concern was to allow historians access to the Dulles' papers.[74]

At the same time, this order corrected an oversight of E.O. 10501. Some agencies which had classified under the Truman order (E.O. 10290) could no longer do so, but no directive spoke to declassification. The new order allowed those stymied agencies to declassify.

A March 9, 1960, memo amended an E. O. 10501 provision which gave any executive agency formed after November 5, 1953, full classification authority. Henceforth, new agencies needed specific presidential

---

[72] Ibid., pp. 803-4.

[73] Ibid., pp. 351-2.

[74] Arkansas Gazette, 9 May 1959, p. 6A.

authorization to classify. That authority was granted eight newly formed agencies.[75]

Executive Order 10901, January 9, 1961, formalized previous changes made by memo and listed the agencies with authority to classify.[76] The formalization was necessary before President Eisenhower left office so the provisions would remain in effect under the new president. Under the order, thirty-two agencies and departments retained full classification authority; 13 others had limited authority.

John F. Kennedy campaigned on a promise to reduce government secrecy. The 1960 Democratic Platform said:[77]

> We reject the Republican Contention that the workings of government are the special private reserve of the Executive. The massive wall of secrecy erected between the Executive branch and the Congress as well as the citizens must be torn down. Information must flow freely, save in those areas in which the national security is involved.

Almost ten years old, the classification system received its first major change. Executive Order 10964,

---

[75] 3 CFR, 1959-63 Comp., p. 805.

[76] Ibid., p. 432.

[77] Emmanuel E. Paraschos, "National Security and the People's Right to Know," (Ph.D. dissertation, University of Missouri-Columbia, 1975), p. 188.

issued September 20, 1961, attempted to stimulate declassification.[78] President Kennedy asked also for press cooperation in a campaign for greater national security in April 1961, while speaking to a meeting of the American Newspaper Association.[79]

> The facts of the matter are that this nation's foes have openly boasted of acquiring through our newspapers information they would otherwise hire agents to acquire through theft, bribery, or espionage.

The order emphasized classification review should be done on a document-by-document, category, program, project or other systematic basis. Classified information would be downgraded or declassified when it no longer needed the level of classification assigned to it.

Also, the order established an automatic declassification and downgrading system. Classified information was placed in one of four categories. Group 1 information was excluded from automatic changes because it originated from a foreign government, was restricted by statute (atomic energy data), or required special handling

---

[78] 3 CFR 1959-63 Comp., pp. 486-9. The information is paraphrased.

[79] Harvard Law Review 85:1197.

(cryptography). Information in Group 2 was designated extremely sensitive by an agency head and therefore exempt from automatic downgrading and declassification. Group 3 contained information needing some degree of protection for an indefinite period. So it was automatically downgraded a level (classification) each 12 years until it reached Confidential but was not automatically declassified. All other information comprised Group 4. Here, classified material was automatically downgraded at 3-year intervals until it reached Confidential, then was declassified after 12 years. The order allowed marking information for earlier declassification.

Once the material was exempted from automatic procedures it was liable to stay classified a long time. The cost and time needed for document review was illustrated when David Cooke, former deputy under secretary of state, told a Congressional committee a review of State Department documents classified prior to 1971 would take 10 years and cost $300,000 annually.[80]

---

[80] U.S., Congress, House, Committee on Government Operations, U.S. Government Information Policies and Practices--The Pentagon Papers (Part 2), Hearings Before a Subcommittee on the Committee on Government Operations, 92d Cong., 1st Sess., 1971, p. 6-1.

E.O. 10964 also added a provision directing agency heads to take "prompt and stringent" administrative action against anyone who disclosed classified information without authorization. The order made some minor changes in handling, marking and transmitting classified information.

Authorized classifying agencies changed names and functions through the years. Three executive orders updated the list of classifiers: E.O. 10985 on January 12, 1962; E.O. 11097 on February 28, 1963; and E.O. 11382 on January 29, 1967.

## Security Classification Studies

During the mid-1950s increasing attention was directed to government security measures, the classification system, and public access to government information. Awareness of problem areas was sparked by the nation's preoccupation with supposed domestic subversion, spy-trials, McCarthy inspired "loyalty-security" investigations and an outbreak of leaks of Pentagon documents. The final straw was a story in the July 12, 1956, New York Times stating the Joint Chiefs of Staff were considering an

800,000 man armed forces reduction by 1960.[81]

On August 13, 1956, Secretary of Defense Charles Wilson, with President Eisenhower's blessing, created a five-member Committee on Classification Information. The committee soon took the name of its chairman, Charles A. Coolidge, Boston lawyer and former assistant secretary of defense. Other panel members were retired general officers representative of the four armed services. Secretary Wilson endowed the committee with a broad though one-sided purpose:[82]

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

The mandate urged the group to consider a review of laws, executive orders and regulations pertaining to classified information, to examine the organization and procedures within the Department of Defense to fix responsibility for unauthorized disclosure of classified information, and to determine the adequacy of measure to prevent such

---

[81] H. Rept. 93-221, p. 16.

[82] Ibid., p. 15.

disclosure.[83]

Since Coolidge Committee instructions did not mention study of overclassification or arbitrary withholding of information, Chairman John Moss of the Special Government Information Committee requested the topics be included on the agenda. The Defense Department assured the congressman the committee probably would do so.[84]

The Coolidge Committee concluded its 3-month study on November 8, 1956. Its report said there was no conscious attempt by Department of Defense personnel to withhold information; further, the classification system was conceptually sound though not operating altogether satisfactorily.[85] Then the bad news: "The two major shortcomings in the operation of the classification system are overclassification and deliberate unauthorized disclosures."[86] The report concluded the primary reason for

---

[83]U.S., Congress, House, Committee on Government Operations, Availability of Information From Federal Departments and Agencies (Part 8), Hearings Before a Special Subcommittee on Government Information, 85th Cong., 1st Sess., 1957, p. 2010.

[84]H. Rept. 93-221, p. 16.

[85]Relyea, p. 859.

[86]H. Rept. 93-221, p. 16.

leaks and casual attitude about the system was overclassification.

The report found a tendency on the part of Pentagon officials to be safe and overclassify without later declassifying information that no longer required protection. Vice Admiral John N. Hoskins, subsequently appointed Director of Declassification Policy, testified before the Moss Committee on November 18, 1957: "...throughout the 180 years of our Government...I have never known a man to be court-martialed for overclassifying a paper, and that is the reason, I am afraid, we are in the mess we are in today...."[87] Such testimony, for its truthfulness, could have been as easily taken yesterday.

The Committee recommended a determined attack on overclassification, including a sharp reduction in the number of people authorized Top Secret classification power. Tough suggestions to plug leaks were offered. Recommended ways to eliminate unnecessary secrecy included appointment of a declassification director, a halt to secrecy changes based on temporary shifts in foreign

---

[87] Ibid., p. 17.

policy and an explanation to the press when information is refused because it is classified. No recommendation called for penalties or disciplinary action in cases of misuse or abuse of classification.

Based upon the study's recommendations, Secretary Wilson issued a new DOD directive (5200.1) on July 8, 1957.[88]

At about the same time, Congress created the Commission on Government Security on August 9, 1955.[89] Los Angeles attorney and former American Bar Association president, Lloyd Wright, was named chairman. The commission's other 12 members were six Democrats and six Republicans. The commission's mandate included study and investigation of the entire Government Security Program, such as the federal-civilian loyalty program, industrial security, atomic energy program, port security, criminal statutes, and the document classification system. The commission held no public hearings but conducted extensive interviews throughout the country.

---

[88]U.S., Congress, House, House Report 1884, 85th Cong., 1st Sess., 1958, pp. 107-16.

[89]Relyea, p. 860.

After nearly two years work, the commission issued a massive 807-page report.[90] The report found some 1.5 million employees of federal departments and agencies had authority to classify documents as of January 1, 1957. The commission wanted to abolish the Confidential classification, criticizing the label's overuse and its restriction on free exchange of scientific and technological information which retards progress necessary to national security. Such abolishment would have meant 76 percent of all State and Commerce information would become public, and 59 percent of all Defense information.[91] The report's conclusion that secrecy inhibited scientific and technological progress took on special relevance when the Soviets launched their "Sputnik." Another recommendation urged creation of a Central Security Office to review and advise on functions of the federal classification program.

The report contained two major controversial

---

[90] Ibid., p. 861.

[91] Norman Dorsen and Stephen Gillers, editors, None of Your Business: Government Secrecy in America (New York: The Viking Press, 1974), p. 67.

portions.[92] The first was an allegation the press often breached security by using classified information in news stories. The charge was not substantiated.

Secondly, the commission urged Congress to

> ...enact legislation making it a crime for any person willfully to disclose without proper authorization, for any purpose whatever, information classified Secret or Top Secret, knowing, or having reasonable grounds to believe, such information to have been so classified.

A $10,000 fine and a five year jail term was the recommended penalty.

Newspaper articles and editorials criticized the recommendations. One article by James Reston of the New York Times pointed out such legislation would have resulted in prosecution of the reporter who uncovered and published Secret documents in the "Teapot Dome" scandal during the 1920s.[93]

---

[92] U.S., Congress, House, Committee on Government Operations, Availability of Information from Federal Departments and Agencies (Part 10), Hearings Before a Special Subcommittee on Government Information, 85th Cong., 1st Sess., 1957, p. 2435.

[93] U.S., Congress, House, Committee on Government Operations, Availability of Information from Federal Departments and Agencies, 85th Cong., 2d Sess., 1958, pp. 15-6.

## Moss Committee

Renewed efforts by scholars, news organizations and legal authorities challenged the government's virtually unlimited power to withhold information from the public. The Coolidge and Wright panels were initiated by the executive, but both were spanned by the Special Government Information subcommittee of the House Government Operations Committee.[94] Headed by Representative John E. Moss of California, the committee began a series of hearings in July 1956.

The Moss subcommittee concentrated heavily on the Defense Department. The subcommittee pinpointed major problem areas which existed almost twenty years ago and specifically recommended corrective actions.[95] They were largely ignored by both Republican and Democratic administrations. The subcommittee concluded:[96]

---

[94]See: H. Rept. 93-221, pp. 21-3; Robert O. Blanchard, "Present at the Creation: The Media and the Moss Committee," Journalism Quarterly 49 (Summer 1972): 272; Wiggins, p. 109.

[95]H. Rept. 85-1884, op. cit., p. 161.

[96]U.S., Congress, House, Availability of Information from Federal Departments and Agencies, 1958, op. cit., p. 152.

> Never before in our democratic form of government has the need for candor been so great. The Nation can no longer afford the danger of withholding information merely because the facts fail to fit a predetermined "policy." Withholding for any reason other than true military security inevitably results in the loss of public confidence--or a greater tragedy. Unfortunately, in no other part of our Government has it been so easy to substitute secrecy for candor and to equate suppression with security.
>
> ...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. ...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.

The subcommittee chastised the Wright Commission for alleging newsmen used stolen classified documents as source material.[97]

> Mr. Wright's indictment of the press is symptomatic of self-styled security experts who point an accusing finger at newsmen for stories which often are based on properly cleared or otherwise publicly available information....

---

[97] Ibid., pp. 154-5.

> No member of the press should be immune from responsibility if sound evidence can be produced to prove that he has in fact deliberately "purloined" and knowingly breached proper classified military secrets.

Though most of its recommendations fell upon deaf ears, the subcommittee did succeed in prodding the Department of Defense into signing a new declassification directive, No. 5200.9. Issued September 27, 1958, the Department's press release stated:[98]

> ...It establishes a new method of which millions of military documents, originated prior to January 1, 1946, and classified Top Secret, Secret, and Confidential will now be downgraded or declassified. The new directive which becomes effective 60 days after signature, automatically cancels, except within a few limited categories, the security classification on millions of documents which no longer need protection in the national interest. In addition, the directive will downgrade to Secret all Top Secret documents which are exempted from declassification.

When the Kennedy administration took office in 1966 subcommittee chairman Moss urged Defense Secretary Robert McNamara to take disciplinary action against overclassifiers.[99] In response, on May 31, 1961, the

---

[98] U.S., Congress, House, Committee on Government Operations, Availability of Information from Federal Departments and Agencies, Progress of Study, H. Rept. 1137, 86th Cong., 1st Sess., 1959, pp. 81-2.

[99] U.S., Congress, Senate, Committee on the Judiciary, Executive Privilege: The Withholding of Information by the

secretary issued DOD Directive 5230-13. The directive formulated four basic principles of public information policy which included:[100]

> Secondly it is essential to avoid disclosures of information that can be of material assistance to our potential enemies, and thereby weaken our defense position. It is equally important to avoid overclassification, and therefore, I suggest that we follow this principle: When in doubt, underclassify. In no event should overclassification be used to avoid public discussion of controversial matters.

However, none but the vaguest administrative penalties ever were implemented against overclassification.

Overclassification abuses inherent in the operation of the executive order classification system were never successfully curtailed. The Moss subcommittee continued its work through legislative attempts to clarify public access to government information. The result was the Freedom of Information Act signed into law by President Lyndon B. Johnson on July 4, 1966.[101]

---

Executive, Hearings Before the Subcommittee on Separation of Powers on S. 1125, 92d Cong., 1st Sess., 1971, p. 33.

[100] U.S., Congress, House, Committee on Government Operations, Availability of Information from Government Departments and Agencies, Progress of Study, H. Rept. 1257, 87th Cong., 1st Sess., 1961, p. 57.

[101] 5 USC 552.

This section has chronologically detailed the origination and early history of the classification system. A system that is rooted in the discretionary power of executive privilege as first used by President Washington, but which has evolved along its own separate path. This section traced the haphazard military use of classifications which became formalized during World War I. The first classification system to encompass all executive government agencies was instituted by President Truman in 1951. There seems to be no single reason for Truman to expand the system outside the military. It was apparently a sign of the insecure times and the real concern that government had to keep some things secret for its own security. This section also summarized President Eisenhower's structuring of the classification system that endured largely unchanged for almost twenty years. This section discussed some of the criticisms of the Truman and Eisenhower systems and the Congressional inquiries prompted by concern for government secrecy.

The next section delineates in some detail the current classification system devised by President Nixon and discusses some of the problems the system has generated. During the early 1970's, renewed concern over the extent

of government secrecy was prompted by activities surrounding the Vietnam War and problems in the operation of the Freedom of Information Act. Both House and Senate Government Operations Committees again became active, holding hearings and conducting investigations.

## CHAPTER III

## EXECUTIVE ORDER 11652

Publication of the Pentagon Papers in June 1971 spurred more than Congressional action.[1] President Nixon revealed an interagency committee had been formed on January 15, 1971, to review classification procedures.[2] The committee was headed by William H. Rehnquist, then an assistant Attorney General, and included representatives from the National Security Council, the Central Intelligence

---

[1] Neil Sheehan, et al., The Pentagon Papers as Published by the New York Times, (New York: Quadrangle Books, 1971), pp. ix-xix. The Pentagon Papers, officially entitled "History of U.S. Decision-Making Process on Vietnam Policy," are a massive top secret history of the United States' role in Indochina. Based on government documents, the study was commissioned by Secretary of Defense Robert McNamara in June 1967. The government sought an injunction to keep the New York Times and Washington Post from publishing the study leaked to them through Rand Corporation employee Daniel Ellsberg, who worked on the study, and Anthony Russo. On June 30, 1971, the Supreme Court by a 6-3 vote freed the newspapers from a temporary injunction and allowed the papers to continue printing the study. See: New York Times v. U.S., 403 US 713; Henkin, Commentary, op. cit.

[2] Relyea, p. 867.

Agency, the Atomic Energy Commission, and the Departments of State and Defense. After Rehnquist's appointment in late 1971 to the Supreme Court, David Young, special assistant to the National Security Council, assumed the chairmanship. One prime goal given the committee was to propose steps to be taken toward speedier declassification.

The project did not seem to have high administration priority. Only after the Pentagon Papers release did meaningful action occur. President Nixon met with the group for the first time on July 1, 1971.[3] Meeting through the summer and fall of 1971, the committee formulated a draft in January 1972 and circulated it for comment by executive agencies. Finally, on March 8, 1972, President Nixon issued Executive Order 11652, "Classification and Declassification of National Security Information and Material." The order became effective June 1, 1972.[4]

In the wake of the Pentagon Papers, historian

---

[3]Alan Diamond, "Declassification of Sensitive Information: A Comment on Executive Order 11652," George Washington Law Review 41 (July 1973):1060.

[4]U.S., President, Executive Order 11652, Federal Register 37, No. 48, 10 March 1972, 5209. The sections of this order are paraphrased, for the full text, refer to the Federal Register.

Arthur Schlesinger, Jr., described the dilemma posed all executives.

> ... You cannot run a government if every internal memorandum is promptly handed to the press. And ... you cannot run much of a press if it is a crime to publish anything stamped secret by the government.[5]

Like presidents before him, President Nixon believed his major reshaping of the classification system served both the interests of the public and the need for governmental secrecy. He outlined the problem in a statement issued with the new order.[6]

> Unfortunately, the system of classification which has evolved in the United States has failed to meet the standards of an open and democratic society, allowing too many papers to be classified for too long a time. The controls which have been imposed on classification authority have proved unworkable, and classification has frequently served to conceal bureaucratic mistakes or to prevent embarrassment to officials and administrations.
>
> The many abuses of the security system can no

---

[5]Arthur Schlesinger, Jr., "The Secrecy Dilemma," New York Times Magazine, 6 February 1972, printed in U.S., Congress, House, Committee on Government Operations, Hearings, U.S. Government Information Policies and Practices -- Security Classification Problems Involving Subsection (b) (1) of the Freedom of Information Act (Part 7), 92d Cong., 2d Sess., 1972, p. 2295.

[6]Ibid., Presidential statement of 8 March 1972, p. 2309.

> longer be tolerated. Fundamental to our way of life is the belief that when information which properly belongs to the public is systematically withheld by those in power, the people soon become ignorant of their own affairs, distrustful of those who manage them, and --- eventually --- incapable of determining their own destinies.

The statement reported the National Archives had 160 million pages of classified documents from World War II and over 300 million classified pages for the years 1946 through 1954.

Testifying before the House of Representatives, J. Fred Buzhardt, Department of Defense general counsel, listed the principle changes wrought by E.O. 11652. The order:[7]

--- reduces the number of departments and agencies authorized to classify; Top Secret classifiers outside the Executive Office of the President were reduced from 24 departments and agencies to 12;

--- restricts classification authority delegation;

--- provides more restrictive guidelines for

---

[7] U.S., Congress, House, Committee on Armed Services, Hearings on the Proper Classification and Handling of Government Information Involving the National Security and H.R. 9853 Before the Special Subcommittee on Intelligence, 92d Cong., 2d Sess., 1972, p. 17387.

classifying;

--- accelerates the downgrading and declassification schedule; automatic declassification after 6-10 years excluding exceptions limited to four specific categories of information; and provides for mandatory review after 10 years for those exempted documents;

--- provides disclosure of classified information after 30 years unless an agency head specifically continues protection.

---gives the National Archives the duty of reviewing and declassifying information classified under previous executive orders and more than 30 years old.

--- allows administrative sanctions against those who abuse the system;

--- establishes an implementation and classification review body, the Interagency Classification Review Committee;

--- defines classified information in terms of "national security" rather than "national defense;"

--- imposes the burden of proof of the need for secrecy on the government.

The order retained three classification categories for information needing protection "because it bears

directly on the effectiveness of our national defense and the conduct of our foreign relations," collectively termed national security.[8] Classified information is defined along a continuum of its significance to national security.

Top Secret refers to national security information whose "unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security."[9] Examples of this damage include

> armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence operations, and the disclosure of scientific and technological developments vital to national security.

The definition concludes with an admonition: "This classification shall be used with the utmost restraint."

Secret refers to national security information whose "unauthorized disclosure could reasonably be expected to cause serious damage to the national security."[10] Examples for this damage level include:

---

[8] Executive Order 11652, Federal Register 37:5209.

[9] E.O. 11652, Sec. 1 (A).

[10] Ibid., Sec. 1(B).

> disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to national security, revelation of significant military plans or intelligence operations, and comprise of significant scientific or technological developments relating to the national security.

And the admonishment this classification should be "sparingly used."

The final classification, Confidential, is reserved for national security information whose "unauthorized disclosure could reasonably be expected to cause damage to the national security."[11] Unlike the higher two classifications, no examples are provided for this damage level.

The three classification definitions generally are more definitive than those provided in previous orders. Implicit in all three is a reasonableness test not found in earlier orders. The Truman and Eisenhower orders spoke only of dangers that "could" or "might" follow unauthorized disclosure. The Nixon administration wanted to emphasize the discretion and judgment involved in assigning a classification. Both Secret and Confidential appear to be more restrictive. The Secret "disruption of foreign

---

[11] Ibid., Sec. 1(C).

relations" seems to require actual rather than potential impairment of such relations as reflected in E.O. 10501's "jeopardizing the international relations" Information classified Confidential must now "cause damage," where before it only had to be "prejudicial to the defense interests of the nation."

The Nixon definition of Top Secret contains some subtle changes from the previous order.[12] The current order, E.O. 11652, slightly broadens the Top Secret definition by substituting "armed hostilities" for the older "armed attack against the U.S. or its allies." Thus, the current order seems to allow for subversive and guerilla activities where the older order did not. Where the previous order specified "a definite break in diplomatic relations," the current order calls for only a "disruption of foreign relations."

Semantic squabbles aside, the whole classification system admits to the weakness always encountered when one person must judge the value of something, here information, to another person. When libertarians cry: "We must have have all information, it will strengthen us;" and the more

---

[12]Diamond, p. 1062.

conservative respond: "Such flagrant breaches in our national security will destroy us;" there is little middle ground.

Yet, for all the reasonableness inherent in preserving national security (by whatever definition), the classification system invites cynicism. Current and past definitions of information protection labels are premised upon degrees of damage prompted by "unauthorized disclosure."[13] If the information is truly critical, any disclosure should be disastrous. But leaks, intentional or unintentional, occur and the Republic has survived. For example, President Johnson conducted an interview with Walter Cronkite on February 6, 1970, in which Johnson read from a Top Secret memo to illustrate his point.[14]

## Semantic Problems

The House of Representatives' Government Information subcommittee was particularly interested in alteration of the wording of two phrases of the Nixon order.[15] While

---

[13] E.O. 11652, Sec. 1.

[14] James McCartney, "What Should Be Secret," Columbia Journalism Review 10 (September/October 1971):41.

[15] H. Rept. 93-221, p. 61.

the old E.O. 10501 specified protected information to be in the "interests of national defense," the current order uses the phrase "interest of the national defense or foreign relations of the United States (hereinafter collectively termed 'national security')."[16] Thus, the current order introduced the more ambiguous words "national security," and used the term "foreign relations." The subcommittee believed the latter term should not have been used, especially because Nixon cited the Freedom of Information Act as legal basis for issuance of his order. But the Act used the term "foreign policy." The subcommittee said the semantic and legal difference between the terms "weaken the entire foundation of E.O. 11652, while failing to correct a basic defect in Executive Order 10501---namely, its lack of a definition for the term 'national defense'."[17]

During the 1972 hearings, William F. Blair, Jr., deputy assistant secretary of state for public affairs, sought to explain the usage by saying: "... I think we tend to regard the word 'policy' in this context and the

---

[16] E.O. 11652, Sec. 1.

[17] H. Rept. 93-221, p. 62.

word 'relations' as being rather minor, but of the two words we would regard relations as being more concrete."[18]

Author of the Freedom of Information Act, Congressman Moss, was not about to forego this little debate. Rep. Moss first made it clear the Freedom of Information Act offered no basis for the executive order, then he said:[19]

> ... We used the term, "defense and foreign policy" very carefully. We did not intend to cover foreign relations. It was proposed but we did not use the term at all because we felt that the foreign relations might be far broader than foreign policy....

On the defensive, Blair declined to specify differences between the two terms. When pressed, he said: "I can only say that in practice we have understood both to be rather broad terms."[20]

Rep. Moss continued:[21]

> We used not foreign relations, we used foreign policy. We had the option of including foreign relations and we also had the option of dealing with national security. We also rejected that

---

[18] U.S., Congress, House, Committee on Government Operations, Hearings, U.S. Government Information Policies and Practices -- Security Classification Problems Involving Subsection (b) (1) of the Freedom of Information Act (Part 7), 92d Cong., 2d Sess., 1972, p. 2468. (Hereinafter: Part 7)

[19] Ibid., p. 2469. [20] Ibid. [21] Ibid.

> as being far more comprehensive than we intended it to be in the act. National defense, rather specific; foreign relations, rather specific. We did not intend either foreign relations or national security.

Rep. Moss brought the discussion back to the reason for this semantic quibbling.

> We are going to have people out here classifying for national security. This is a quick judgment like that. We are going to classify or we are not going to classify. This is an ill-defined term and you tell me that you can go away from this room and sit down and give very careful thought to it and you think you can come up with a definition of what is involved in national security. Remember, the man who is classifying is going to have to do this every time that a paper comes before him.[22]

This May 1972 discussion followed questions posed about "national security" in the wake of the Pentagon Papers. The congressmen, at least, apparently foresaw the broad application, indeed, of the term and what it would encompass during President Nixon's Watergate days.[23]

---

[22] Ibid., p. 2470.

[23] Now known simply as "Watergate," the term refers to a break-in of Democratic National Committee offices in the Washington apartment/office complex named Watergate by a special team (the "plumbers") under White House control on June 17, 1972. Succeeding events culminated in the resignation of President Richard M. Nixon on August 9, 1973. See chronology in Sylvia Westerman, ed., The CBS News Almanac 1976 (Maplewood, N.J.: Hammond Almanac, Inc., 1975), pp. 1038-9.

J. Fred Buzhardt, Department of Defense general counsel, who was testifying with Assistant Secretary Blair May 2, later provided a statement defining national security.

> As used in Executive Order 11652, the term "national security" is explicitly used in a collective sense to encompass "national defense" and "foreign relations." In my personal opinion, "national security," as used in this context, is synonymous with the generally understood definition of "national defense" as used in Executive Order 10501. In this context, "national security" is a generic concept of broad connotations referring to the Military Establishment and the related activities of national preparedness including those diplomatic and international political activities which are related to the discussion, avoidance or peaceful resolution of potential or existing international differences which could otherwise generate a military threat to the United States or its mutual security arrangements.[24]

To add credence to the term's usage, Buzhardt reported "national security" appears more than 164 times in the United States Code, 1964 edition. Congress used the term in Public Law 92-68, enacted August 6, 1971, calling for annual aeronautics reports when it specified reports are to exclude "...information which has been classified for reasons of national security."

---

[24] Part 7, p. 2470.

The Buzhardt statement concluded:[25]

> It is significant that although Executive Order 10501 used the term "national defense," the Congress chose to use the words "national security" in describing classified information.

Complicating the supposed straightforward classification system, various departmental implementing regulations attempt to define properly classified information. Department of Defense regulations emphasize the judgment factor.[26]

> Classification is a balanced judgment. There must be a positive basis for classification, but both advantages and disadvantages to classify must be considered. Determination to classify shall not be applied until after full consideration of both aspects.

A set of criteria is then presented. The document is not classified until each criterion is considered. The regulation says information is properly classified if it:

---is sensitive, or when read with other information would reveal sensitive information;

---provides the United States with "scientific, engineering, technological, operational, intelligence, strategic or tactical advantage directly related to

---

[25] Ibid.

[26] 32 CFR, sec. 159.202, July, 1976.

national security";

---would weaken U.S. war of defense capabilities.

The regulation does not ask the classifier to consider the public's need for information before classifying.

## Downgrading and Declassifying

The major innovation of Executive Order 11652 is in the rules governing downgrading and declassification.[27] A general declassification schedule (GDS) automatically downgrades and eventually declassifies information at fixed time intervals, doing away with the complicated group system.

Top Secret information becomes Secret at the end of the second calendar year after its classification. It is reduced to Confidential after two more years and declassified after another six years. Confidential information is declassified six years after origin. So, classified information becomes declassified after 10, 8 or 6 years according to its national security significance. A genuinely automatic system is outlined.

Except, and there are always exceptions, the system

---

[27] E.O. 11652, sec. 5.

does not apply to all classified information. Section 5 (B) of the order recognizes some information "may warrant some degree of protection for a period exceeding that provided in the general declassification schedule." Officials with original Top Secret classification authority may exempt from the GDS any level of classified information under his supervision if it falls within one of four categories.

> (1) Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.
> (2) Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.
> (3) Classified information or material disclosing a system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security.
> (4) Classified information or material the disclosure of which would place a person in immediate jeopardy.

The order requires exemptions to be kept to an "absolute minimum consistent with national security requirements."

Some agencies apparently believe most of their classified information needs extra protection. During 1973 and into 1974, the Central Intelligence Agency exempted 96 percent of its classified documents from the

declassification schedule.[28]

The Department of Defense, CIA and the Energy Research and Development Administration are excluded from Interagency Classification Review Committee reports because most of their classified material is exempt from automatic declassification.[29] However, in 1976, 75 percent of documents classified by other executive branch departments were placed in the general declassification schedule. The amount of classified material exempted has increased slowly the past three years.[30]

In applying the GDS to papers classified under the pre-Nixon system, only information from Group 4 (to be systematically declassified after 12 years) is included. All other classified papers remain excluded though they are subject to mandatory review after ten years. All

---

[28] U.S., Congress, Senate, Committee on Government Operations, Government Secrecy, Hearings Before the Subcommittee on Intergovernmental Relations, 93rd Cong., 2d Sess., 1974, p. 102.

[29] Interagency Classification Review Committee, 1976 Progress Report, by James B. Rhoads, Acting Chairman (Washington, July 1977), p. 21.

[30] Ibid., pp. 21-2.

exempted information can be reviewed by the originator after ten years if three conditions are met: "(1) a department or member of the public requests a review; (2) the request describes the record with sufficient particularity to enable the Department to identify it; and (3) the record can be obtained with only a reasonable amount of effort."[31] If the material no longer qualifies for exemption, it will be declassified. Requests for reviews increased 90 percent in 1976 over the previous year.[32]

Dr. James B. Rhoads, Archivist of the United States, is optimistic about the review procedure.[33]

> ...Those documents in our holdings which we, ourselves, acting under agency guidelines cannot declassify, can be sent to the agencies, who must act upon them and who must act with reasonable speed. We believe that this provision will lead to the opening of significant quantities even of fairly recent classified material.

The order states all classified information, regardless of its origin, will be declassified after 30 years. Any exemption must be sought personally in writing

---

[31] E.O. 11652, sec. 5 (C).

[32] ICRC, 1976 Progress Report, p. 1.

[33] Part 7, p. 2606.

by a department head. That individual must show continued protection is essential to the national security or would place a person in immediate danger. If the exemption is continued, the period of continued classification must be indicated. The Archivist receives the burden of reviewing for declassification information classified before E.O. 11652. To date approximately 200 million pages have been declassified, about 30 million of that during 1976.[34]

The order brings presidential libraries under the classification system for the first time.[35] Rule-making and enforcement powers are left to regulatory bodies.[36]

## Interagency Classification Review Committee

A new entity, the Interagency Classification Review Committee (ICRC), was created to assist the National Security Council in implementing and monitoring the order.[37] The National Security Council issued a

---

[34] ICRC, 1976 Progress Report, p. 25.

[35] Barker, p. 20.

[36] E.O. 11652, sec. 6 (A).

[37] Ibid.

directive providing specific guidance and elaboration on E.O. 11652.[38] The ICRC has one representative each from the Departments of State, Defense and Justice, the Atomic Energy Commission, the CIA, the National Security Council Staff and the Archivist of the United States.[39] Its first chairman, presidentially appointed, was John S. D. Eisenhower.[40]

E.O. 11652 directs the ICRC to meet regularly and to perform three functions:[41] (1) oversee agencies to insure compliance with the order and implementing directive; (2) receive, consider and act on suggestions and complaints about administration of the order; (3) receive from the agencies any material needed to carry out its functions.

---

[38]U.S., National Security Council, "National Security Council Directive Governing the Classification, Downgrading, Declassification and Safeguarding of National Security Information," Federal Register 37, 19 May 1972, 10053.

[39]This is the composition of the ICRC after the Archivist was added by Executive Order 11714, 24 April 1973.

[40]Washington Post, 18 May 1972.

[41]E.O. 11652, sec. 7 (A).

The security council directive added some responsibilities:[42]

> (a) prevent overclassification, (b) insure prompt declassification in accord with the provisions of the order, (c) facilitate access to declassified material and (d) eliminate unauthorized disclosure of classified information.

The ICRC's power is real. Each organization's implementing regulations must be approved by the committee. Recognizing bureaucratic reluctance to invoke administrative remedies, the committee requires detailed statistical reports from all classifying agencies.[43] These reports cover seven areas.

(1) Original classifying authorities --- are listed semiannually by name and title with a total for each agency; the hope is for a decreasing number of classifiers and an increasing quality of classification.

(2) Classification abuses and administrative security violations --- includes overclassification, unnecessary classification, unnecessary exemption or exemption without

---

[42] National Security Council Directive, sec. IV C.

[43] For a listing of current reporting requirements see Federal Register 42, 13 January 1977, 2679.

authority; this semiannual report is a measure of the effectiveness of the classification program.

(3) Unauthorized disclosures --- are the transfer of classified information to an unauthorized person; six disclosures were reported in 1976, most the result of articles in the press.

(4) Mandatory declassification review actions --- is a semiannual report used to monitor requests for review of classified information more than ten years old; if the document is less than ten years old and the originating agency has no objection, the committee may review it.

(5) Annual review list -- includes classified material not scheduled for automatic declassification.

(6) Annual declassification list --- is a two part listing of documents declassified that calendar year and those documents on the Annual review list determined to be declassified.

(7) Semiannual summary --- provides a statistical summary covering the volume of documents classified, efforts to increase public access to declassified information, and efforts to improve management of classified material. Because of the volume of classified material, some departments such as DOD are allowed to use sampling

procedures for this summary.

The ICRC has succeeded quite well, considering the staff consisted of two persons until 1976.[44] The staff, now eight, receives assistance from the National Archives. All committee members are full-time employees of the agencies they represent. Regular on-site program reviews of information security programs began in 1976.

The committee acts as the appeal authority for denials of declassification requests to departmental committees. Most appellants are historical researchers who started the process at presidential libraries. Nine of 11 appeals were accepted for review during 1976.[45] In six cases the requested information was partially declassified over objections by the departments. Is that a sign of success for the committee in promoting public access? Or is it indicative of failure on the part of departmental committees?

Just over half the appeals brought to the ICRC overturned departmental decisions to some extent. How much information would have been released if more

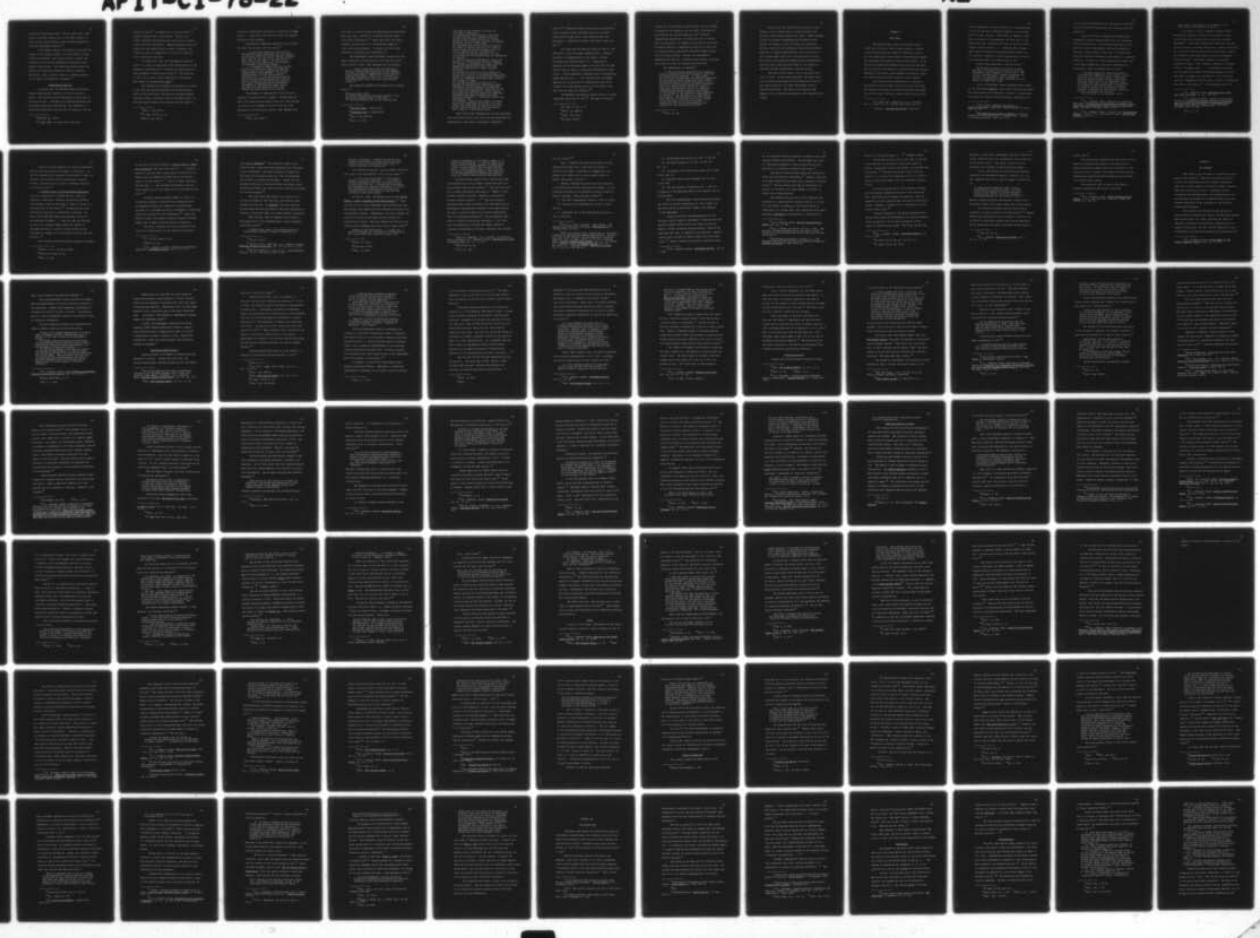
---

[44] ICRC, 1976 Progress Report, p. 7.

[45] ICRC, 1976 Progress Report, p. 27.

AD-A051 506 AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OHIO F/G 5/4
THE NATIONAL SECURITY CLASSIFICATION SYSTEM.(U)
DEC 77 R L OBORN
UNCLASSIFIED AFIT-CI-78-22 NL

2 OF 3
AD A051 506



researchers had pressed their claims to ICRC level? The system's greatest promise lies in the ICRC's ability to check classification abuses at their source through the required departmental reports.[46]

In the appeal process, the ICRC must determine the nature of the document sought, its relationship to other classified documents, the timing of public release upon declassification and any interagency disagreement about proper classification. The classifying agency bears the burden of proving the information requires continued protection. Only a majority vote of a committee quorum (7) is needed to declassify a document.[47]

## Congressional Reaction

As we have seen, the Pentagon Papers publication sparked Congressional inquiries as well as executive action. The executive had the advantage of being able to move more quickly. Chairman of the Foreign Operations and Government Information subcommittee, Rep. Moorhead, was particularly perturbed with the time of release of the new

---

[46] Diamond, pp. 1063-4.

[47] 32 CFR, Chapt. 20, Part 2000, July 1976.

executive order.[48] It seemed to him to be an effort to undercut Congressional investigation. The security council implementing guideline was issued only two weeks before the order took effect. Agency regulations were not ready until two months after the order's issuance, providing no time for preparation or training of those who had to administer the order.

On January 24, 1972, the subcommittee announced plans for a series of hearings on the administration of the Freedom of Information Act, including an investigation of the government's classification system.[49] The order was at that time in final review stages and its provisions were leaked to the Washington Post.[50]

The subcommittee attempted unsuccessfully to obtain a copy from the Justice Department and the White House. Later on the House floor, subcommittee chairman Moorhead recounted efforts to obtain a copy of the draft order, but cautioned against hasty action because of what seemed to

---

[48] Part 7, pp. 2844-5.

[49] H. Rept. 93-221, p. 52.

[50] Part 7, pp. 2303-6.

be serious inadequacies and defects revealed by the Post article. A week later the order was issued and promptly deplored by Rep. Moorhead.

Representative Moorhead expressed his ire before the House the day the order was issued.[51]

> ... We politely sought the final draft of the Executive order last month, but the request was politely denied as none of Congress' business until the last nail was driven into the coffin. Well, that is all right --- we reserve the right to bury the coffin with a law passed by the Congress of the United States.
>
> ... I thought the House would like to know we plan to continue our public hearings and hope to come up with a proposed law for the consideration of the Congress. It was the Congress which initiated the Freedom of Information Act --- not the executive branch. And we believe Congress should now bring into reality a practical classification law which will insure the maximum flow of Government information to the American people while at the same time protecting the truly vital defense and state secrets of our Nation.

The prophecy of Congressional action could not overcome the executive fait accompli. The hearings had dealt with classification abuses under E.O. 10501 and now, in fairness, must attempt to decide if the new order adequately corrected earlier abuses. Rep. Moorhead was

---

[51] Ibid., pp. 2848-9.

not ready for reconciliation and expressed grave misgivings about the order, calling it "a shoddy technical effort" with "major deficiences."[52] Three days after the order's issuance, he described it to the Washington Post as a "very restrictive document. It appears to be an order written by classifiers for classifiers."[53]

The subcommittee staff thoroughly analyzed the new order, comparing its provisions on a section-by-section basis with E.O. 10501. Rep. Moorhead said the analysis

> ... clearly shows why I had urged the White House to make available the draft of the proposed new order so that our subcommittee could informally suggest improvements, based on our many years of oversight experience in this area, to really deal with root causes of the security classification problem.[54]

The Moorhead subcommittee recognized the following defects.[55]

> Executive Order 11652:
> (1) Totally misconstrues the basic meaning of the Freedom of Information Act (5 USC 552);
> (2) Confuses the sanctions of the Criminal Code

---

[52] New York Times, 22 March 1973.

[53] Washington Post, 11 March 1972.

[54] Part 7, pp. 2849-83.

[55] Ibid., p. 2850.

that apply to the wrongful disclosure of classified information;
(3) Confuses the legal meaning of the terms "national defense" and "national security" and the terms "foreign policy" and "foreign relations" while failing to provide an adequate definition for any of the terms;
(4) Increases (not reduces) the limitation on the number of persons who can wield classification stamps and restricts public access to lists of persons having such authority;
(5) Provides no specific penalties for over-classification or misclassification of information or material;
(6) Permits executive departments to hide the identity of classifiers of specific documents;
(7) Contains no requirement to depart from the general declassification rules, even when classified information no longer requires protection;
(8) Permits full details of major defense or foreign policy errors of an administration to be cloaked for a minimum of three 4-year Presidential terms, but loopholes could extend this secrecy for 30 years or longer;
(9) Provides no public accountability to Congress for the actions of the newly created Interagency Classification Review Committee;
(10) Legitimizes and broadens authority for the use of special categories of "classification" governing access and distribution of classified information and material beyond the three specified categories --- Top Secret, Secret and Confidential; and
(11) Creates a "special priviledge" for former Presidential appointees for access to certain papers that could serve as the basis for their private profit through the sale of articles, books, memoirs to publishing houses.

What rankled Rep. Moorhead most was the undeniable fact the executive had struck first and had maintained his preeminence in the field of government information

control.[56] Claiming the hasty unveiling of new executive order procedures would "adversely affect our national defense and foreign policy," Rep. Moorhead asked the President to "indefintely suspend" the order's effective date.[57]

The order gave the National Security Council, with ICRC help, overall oversight responsibility. Congress believed, as representative of the people, ultimate accountability should belong to it. Congressional questions during hearings sought to discover how the ICRC would be open to public scrutiny and Congressional supervision. A State Department spokesman gave an unreassuring answer when he said, "... the committee like its member agencies will be sensitive to congressional and public interest in its performance and will do its best to see that both are kept well informed."[58]

The Moorhead subcommittee finally issued its uncomplimentary report May 22, 1973.[59] The panel reiterated

---

[56] H. Rept. 93-221, p. 55.

[57] Ibid., pp. 2889-90.

[58] Ibid., pp. 2516-7.

[59] H. Rept. 93-221.

certain E.O. 11652 defects, noted Congress was not allowed to comment on the design of the new order, chastised the executive for not allowing agencies time to prepare implementing regulations, criticized the lack of clarity about classification of "domestic surveillance" activities be federal agencies, disapproved limitations on World War II classified data, and praised the Atomic Energy Commission's statutory system. Finally, the subcommittee emphasized the need for a vigorous review system, including full judicial review of classification decisions.

The subcommittee recommended:[60]

> ... That legislation providing for a statutory security classification system should be considered and enacted by the Congress. It should apply to all executive departments and agencies responsible for the classification, protection, and ultimate declassification of sensitive information vital to our Nation's defense and foreign policy interests. Such a law should clearly affirm the right of committees of Congress to obtain all classified information held by the executive branch when, in the judgment of the committee, such information is relevant to its legislative or investigative jurisdiction. The law should also make certain that committees of Congress will not be impeded in the full exercise of their oversight responsibilities over the administration and operation of the classification system.

---

[60] Ibid., p. 104.

This section has specifically outlined the major features of the current executive order governing the security classification system, E.O. 11652. Those features include an automatic downgrading and declassification system, an attempt to limit the number of classifiers and the creation of the Interagency Classification Review Committee to oversee administrative functions and act as the ultimate appeal board for classification decisions. This section also mentioned Congressional dissatisfaction with the order itself and the timing of its release to seemingly preempt Congressional statutory action.

The next section takes a look at the legal basis of E.O. 11652. As previously mentioned, the legal roots for a classification system are not explicitly stated in the Constitution but lie within the broader claim of executive privilege. The next section explores what appears to be a statutory acceptance of the classification system.

## CHAPTER IV

## LEGAL BASIS

The Pentagon Papers and the Watergate scandal forced the citizenry to more closely consider a bloated secrecy system which has eroded our democratic society. Cold War paranoia and valid defense considerations spawned the government-wide secrecy classification system. It was generally accepted that people should trust the president and his advisors with matters of foreign policy and defense. Subsequent revelations caused Congress to question closely the justification and legal basis for such a system.[1]

The classification system gains its legitimacy originally from the broader claim of executive privilege. The Constitution explicitly authorizes neither the system nor the privilege.[2] The only constitutional article which

---

[1] See, generally: Henkin, op. cit.; Paraschos, op. cit.; Cox, op. cit.; Dorsen and Gillers, op. cit.

[2] "Project," Michigan Law Review 73:998-1005.

requires Congress to inform the public of its proceedings is also the one which authorizes Congress to use secrecy. Article I says, in part: "Each house of Congress shall keep a journal of its proceedings, and from time to time publish the same, excepting such parts as may be in their judgment require secrecy ...." Professor Raoul Berger, a legal expert on executive privilege, believes failure by the drafters to require a similar presidential action was an intentional denial of secrecy power to him.[3]

Harold Cross maintained a similar belief.[4]

> The executive branch as of now has no such specially privileged right of privacy as against the people, their Congress or their courts. The claim to one harks back to royal prerogative and is made in a land where, there is reason to believe, the people have done something more than merely to change their kings.

Clark R. Mollenhoff, former Washington Bureau Chief for the Des Moines Register, more bluntly and less charitably described executive privilege not a myth but "a naked power grab under the cloak of constitutionality, thoroughly evil

---

[3]Raoul Berger, Executive Privilege: A Constitutional Myth (Cambridge: Harvard University Press, 1974), p. 205.

[4]The Executive Privilege to Withhold, Freedom of Information Center Report No. 9 (Columbia, Mo.: Freedom of Information Center, 1958), pp. 1-3.

in its origins and destructive to any effort to make the executive branch accountable for the laws passed by this Congress."[5]

The great conflict prompting such impassioned statements involves Congressional access to information held by the executive. Even Richard Nixon early in his political career spoke against executive withholding. President Truman refused to turn over to the House Un-American Activities Committee an FBI report on a prominent scientist. On April 22, 1948, Representative Nixon rose in the House chamber and conclusively denounced the presidential right to withhold when he said:[6]

> I say that proposition cannot stand from a constitutional standpoint or on the basis of the merits for this very good reason: That would mean that the President could have arbitrarily issued an Executive Order in the Meyers case, the Teapot Dome case, or any other case denying the Congress of the United States information it needed to conduct an investigation of the executive department and the Congress would have no right to question his decision.
>
> Any such order of the President can be

---

[5]U.S., Congress, House, Committee on Government Operations, Availability of Information to Congress, Hearings Before a Subcommittee on H.R. 4938, H.R. 5983, H.R. 6438, 93rd Cong., 1st Sess., 1973, p. 81.

[6]U.S., Congress, House, 22 April 1948, Congressional Record, p. 4783, cited in Dorsen and Gillers, None of Your Business, pp. 28-9.

questioned by the Congress as to whether or not that order is justified on the merits.

In a March 12, 1973, statement President Nixon asserted the doctrine of executive privilege is rooted in the Constitution and was first invoked by President Washington.[7] Some legal scholars and historians find this historical basis to be mere fabrication. Arthur Schlesinger, Jr., could not find the term "executive privilege" used by any President or Attorney General before the Eisenhower administration.[8] Schlesinger referred to President Eisenhower's May 17, 1954, letter to Secretary of Defense Wilson. Eisenhower wrote: "... throughout our history the President has withheld information whenever he found that what was sought was confidential or its disclosure would be incompatible with the public interest or jeopardize the safety of the Nation."[9] An accompanying memo from

---

[7] U.S., Congress, House, Hearings on H.R. 4938, H.R. 5983, H.R. 6438, op. cit., pp. 75-7.

[8] U.S., Congress, Senate, Committee on Government Operations, Executive Privilege--Secrecy in Government, Hearings Before the Subcommittee on Intergovernmental Relations on S. 2170, S. 2378, S. 2420, 94th Cong., 1st Sess., 1975, p. 241.

[9] Ibid., p. 225.

Attorney General Herbert Brownell claimed lengthy historical precedent for an executive privilege. Actually, it wasn't until 1835 during the presidency of Andrew Jackson that there was an unequivocal assertion of a constitutionally derived discretionary power to withhold information from Congress.[10]

The constitutional basis for executive information withholding is by no means firm. The constitutional grant of power is only implied. Article II of the Constitution states: "The executive power shall be vested in a President of the United States of America." The last clause in Section 3 of the same article continues: "He shall take care that the laws be faithfully executed." Further, the article empowers the president to conduct foreign relations and to maintain the national defense as Commander in Chief of the armed forces.

Article II's implications lead us away from any broad discretionary executive privilege toward the more narrow duty to preserve potentially harmful information about foreign and military affairs. In its 1957 report,

---

[10]Norman Dorsen and John H.F. Shattuck, "Executive Privilege, the Congress and the Courts," Ohio State Law Journal 35 (1974, No. 1):12.

the Commission on Government Security said:[11]

> When these provisions of Article II are considered in light of existing Presidential authority to appoint and remove executive officers directly responsible to him there is demonstrated the broad Presidential supervisory and regulatory authority over the internal operations of the Executive Branch. By issuing the proper Executive or administrative order he exercises this power of direction and supervision over his subordinates in the discharge of their duties. He thus "takes care" that the laws are being faithfully executed by those acting in his behalf; and in the instant case the pertinent laws would involve espionage, sabotage, and related statutes, should such Presidential authority not be predicated upon statutory authority or direction.

Rep. John N. Erlenborn specifically divorced the classification system from the more onerous, broader executive privilege when he said,

> The point here is not to confuse executive privilege with classification of information. I think the purpose of the two is altogether different.
>
> Classification of information is for the purpose of keeping secret things that might endanger the United States. The executive privilege is exercised only to protect the right of the President or an agency head to get advice free from the constraints that would exist if that advice became a matter of controversy.[12]

---

[11] Part 7, cited in Department of Justice response to questions, p. 2824.

[12] U.S., Congress, House, Availability of Information to Congress, p. 17.

Executive branch authority to classify information has not been successfully challenged in the courts. In 1875 the Supreme Court recognized the President's power to protect vital national security information, provided neither a legislative nor a judicial subpoena restricts his ability to act.[13]

In United States v. Curtiss-Wright Corporation, the Court stated that in foreign affairs, "with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation."[14] Recognizing the broad presidential function in international relations, the Court could understand where the President, acting on the government's behalf, "... has the right and the duty to strive for internal secrecy about the conduct of governmental affairs in areas in which disclosure may reasonably be thought to be inconsistent with the national interest."[15]

The President received similarly expansive deference

---

[13] Totten v. U.S., 92 US 105 (1875).

[14] 299 US 304 (1936) at 319.

[15] Ibid., at 320.

in the area of national defense in C&S Air Lines v. Waterman Corporation, when the Court said the " ... President ... possess in his own right certain powers conferred by the Constitution as Commander-in-Chief and as the Nation's organ in foreign affairs."[16] Acting in these capacities, the President "... has available intelligence services whose reports are not and ought not to be published to the world."[17]

Assistant Attorney General Robert G. Dixon, Jr., linked the President's constitutional responsibilities as Commander-in-Chief and conductor of international relations to a presidential power to establish a classifying system for national security information.[18] Dixon said Executive Order 11652 merely instructed executive branch members how to handle national security information.

The Court recognized not only the power but the reality of classification in the leading state secrets

---

[16] 333 US 103 (1948) at 109.

[17] Ibid., at 111.

[18] U.S., Congress, Senate, Committee on Government Operations, Government Secrecy, op. cit., p. 143.

case U.S. v. Reynolds.[19] The plaintiff sought an Air Force accident report which the government said contained secret information. The Court recognized a common law privilege for military secrets and ruled the government did not have to release the documents. Though the Court extended protection to national defense information under executive privilege, the executive had to show the privilege was invoked properly.[20]

The court found some control over executive discretion was needed by the judiciary, particularly where evidence was involved. In Reynolds, the Court believed the government had met the burden of proof by submitting an affidavit stating the report was indeed properly classified.

More recently, when the Supreme Court refused to stop publication of the Pentagon Papers, Justice Marshall, concurring, wrote:[21]

> In these cases, there is no problem concerning the President's power to classify information as

---

[19] 345 US 1 (1953).

[20] 345 US 1 at 10. Also see: U.S., Congress, Senate, Hearings, Executive Privilege, vol. III, op. cit., p. 205.

[21] New York Times Co. v. U.S., U.S. v. The Washington Post Co., et al., 403 US 713 (1971) at 741.

> Secret or Top Secret. Congress has specifically recognized Presidential authority which has been formally exercised in Executive Order 10501 to classify documents and information.

In a concurring opinion, Justice Stewart recognized the source of the presidential classification power.[22]

> ... 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.

On July 24, 1974, the Supreme Court decided United States v. Nixon, President of the United States.[23] Nixon lost his suit to retain subpoenaed tape conversations with White House staff members who were allegedly associated with the Watergate burglars. Nonetheless, the Court affirmed the doctrine of executive privilege and the validity of a classification system. The Court endowed the doctrine with constitutional grounding when Chief Justice Berger wrote:[24]

> Nowhere in the Constitution ... is there any explicit reference to a privilege of confidentiality, yet to the extent this interest relates to the

---

[22] Ibid., at 729-30.

[23] 418 US 683 (1974).

[24] Ibid., at 705-6.

> effective discharge of a President's powers it is constitutionally based .... The privilege can be said to derive from the supremacy of each branch within its own assigned areas of constitutional duties. Certain powers and privileges flow from the nature of enumerated powers: the protection of the confidentiality of Presidential communications has similar constitutional underpinnings.

President Nixon asserted only a general privilege of confidentiality in his attempt to keep the tapes, not that national security was involved.[25] The Court was careful to observe the matter came before it "absent a claim of need to protect military, diplomatic or sensitive national security secrets ...."[26] The Court balanced President Nixon's plea to preserve the confidentiality of presidential conversations contained in the tapes against the need to provide evidence in a criminal prosecution, that of the Watergate burglars.[27] But by observing that a claim of national security was not before it, the Court left the impression it accords the highest degree of privilege to presidential military, diplomatic and national

---

[25] John H.F. Shattuck, "U.S. v. Nixon: A Dissenting View," printed in U.S., Congress, Senate, Hearings on S. 2170, S. 2378, S. 2420, op. cit., p. 262.

[26] 418 US 683 at 706.

[27] 94 S. Ct. 3106.

security affairs.[28]

Thus, it appears the courts have dealt with and recognized the basis for a classification system --- executive privilege. In the New York Times case, the Supreme Court agreed such a system seemed logical to protect the nation's security.

However, Congress has never explicitly provided a government-wide security classification system. It has recognized the need for or existence of such a system in numerous statutes. Those statutes include:[29]

(1) The 1789 "housekeeping" statute, 5 USC 22 (1789);

(2) Sections of the Espionage Act of 1917, 18 USC 792-798;

(3) Subsection (b) of the Internal Security Act of 1950, 50 USC 783;

---

[28] 94 S. Ct. 3109. Also see: Raoul Berger, "The Incarnation of Executive Privilege," UCLA Law Review 22 (October 1974): 4, 26-9.

[29] This list results from a compilation of information presented by executive and Congressional sources. For the full text of the statutes, see the appropriate reference. Generally, see: H. Rept. 93-221, p. 11; U.S., Congress, House, Security Classification Reform, op. cit., pp. 289-94; U.S., Congress, Senate, Government Secrecy, op. cit., pp. 146-8; U.S., Congress, Senate, Executive Privilege, vol. I, op. cit., pp. 458-60.

(4) The National Security Act of 1947, 50 USC 401;

(5) The Atomic Energy Act of 1954, 42 USC 2162, sec. 142;

(6) Provisions of the Foreign Assistance Act of 1961, 22 USC 2394 (b);

(7) The Arms Control and Disarmament Act of 1961, 22 USC 2585;

(8) And the Freedom of Information Act, 5 USC 552. A summation of the pertinent part of each stature will be provided here.

The 1789 "housekeeping" statute authorized department heads to *provide regulations for* "the custody, use and preservation of the records, papers, and property of the department ...."

Sections 792-798 of the Espionage Act of 1917 recognize certain types of information "connected with the national defense" which could cause injury to the U.S. Robert G. Dixon, assistant attorney general, believed the espionage laws made "it imperative to establish a classification system in order to enforce them fairly and effectively."[30] The Act granted the President authority during

---

[30]U.S., Congress, Senate, Government Secrecy, op. cit. p. 148.

war or proclaimed national emergency to prohibit entry into national defense installations. The espionage laws refer to "classified information," thus giving notice of the existence of an executive classification system.[31]

The courts recognized some system was necessary to allow fair and effective enforcement.[32] However, there are no criminal penalties predicated upon a document's classification.[33] The laws concern the type of information contained in a document, not simply whether a document is marked with a classification.

The Internal Security Act of 1950 recognizes the existence of a classification system by making it a crime "for any officer or employee of the United States" to communicate to a foreign agent "any information which shall have been classified by the President as affecting the

---

[31]U.S., Congress, House, Security Classification Reform, op. cit., p. 289.

[32]U.S. v. Heine, 151 F2d 813 (2d Cir., 1945). The decision intimated information was not subject to the protection of the Espionage Acts unless the executive had classified it.

[33]Harold Edgar and Benno C. Schmidt, Jr., "The Espionage Statutes and Publication of Defense Information," Columbia Law Review 73 (May 1973):931.

security of the United States ...."[34] (Emphasis added.)

The National Security Act of 1947 made it the duty of the Director of the Central Intelligence Agency to protect "intelligence sources and methods from unauthorized disclosures."[35] The provision doesn't specify how the Director is to fulfill his responsibility, but a classification system could emanate from this statutory responsibility.

The Atomic Energy Act of 1954 recognizes defense and intelligence information as part of the "restricted data" affecting nuclear weapons and material. This Act represents the only Congressional statutory classification system. Congress is pleased with its operation, as will become evident later.[36]

Oblique references in the Foreign Assistance Act and the Arms Control and Disarmament Act indicate Congressional recognition, if not total acceptance, of the executive classification system. The former obliges the

---

[34]U.S., Congress, Senate, Government Secrecy, op. cit., p. 148.

[35]61 Stat. 495 at 498, sec. 102 (d) (3).

[36]H. Rept. 93-221, pp. 96-9.

President to make public Development Loan Fund information unless "deemed by him to be incompatible with the security of the United States." The latter requires security clearances for personnel of the Arms Control Agency.

Lastly, the Freedom of Information Act expressly recognizes the presidential system in exemption (b) (1). That exemption says the Act does not apply to matters that are

> (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order.[37]

However, nothing precludes Congressional classification legislation which could largely repeal the current system.

The executive national security classification system has no explicit bases in the Constitution.[38] However, Congress has acquiesced to such a system by confining its activities to providing criminal sanctions and penalties and by recognizing the need and existence of the system in

---

[37] 5 USC 552 (b) (1).

[38] U.S., Congress, Executive Privilege, vol. 1, op. cit., p. 460.

various laws.[39]

This section has considered the legal basis for an executive classification system in the Constitution's implied presidential powers and court recognition of the validity of such a system. This section briefly reviewed Congressional legislation which recognizes the existence of a classification system.

The study now turns to some of the numerous problems generated by the system's operation.

---

[39]U.S., Congress, House, Security Classification Reform, op. cit., pp. 289, 499. Also see: Edgar and Schmidt, Jr., op. cit.

## CHAPTER V

## THE PROBLEMS

The conflict over the amount of government secrecy has not been resolved.[1] What was originally a military concern for safeguarding sensitive defense information grew into a system capable of hiding from public view more than strictly military secrets. Government actions surrounding the Pentagon Papers, the Ellsberg-Russo trial and Watergate contributed to a hightened sensitivity and broader realization of the dimensions of the security classification problem.

This section will discuss the multiplicity of abuses caused by previous and current classification systems. The current order, E.O. 11652, specifies the number of approved classifiers but bureaucratic loopholes tend to negate the provision. We will view the magnitude of over-classification and the way declassification procedures can

---

[1] U.S., Congress, Senate, Final Report of the Select Committee, Book VI, op. cit., p. 349.

be circumvented by exemption. The enormous costs created by these abuses will be explored. Lastly, the section looks at the sanctions provided by the current order and their ineffectiveness in dealing with internal abuse and unauthorized disclosure.

## Volume

The sheer bulk of classified documents is difficult to comprehend. The volume has increased so greatly during the past 30 years no one really knows just how many classified documents exist. For example, William G. Florence, a retired Air Force security classification expert with 43 years Federal service, estimated the Department of Defense had in June 1971, "at least 20 million classified documents, including reproduced copies ...."[2]

Later in the 1971 House hearings by the Government Information subcommittee, David O. Cooke, deupty assistant secretary of defense, first said there was no way of knowing

---

[2]U.S., Congress, House, Committee on Government Operations, Hearings, U.S. Government Information Policies and Practices--The Pentagon Papers (Part 1), 92d Cong., 1st Sess., 1971, p. 97. (Hereinafter: Part 1).

how many classified documents DOD had.[3]

> No reports are required at this time of the number of classified documents maintained by every DOD activity. The closest we can come to it ... is biennial record reports indicating DOD holdings in total, classified and unclassified, of approximately 6 million cubic feet [about 12 billion sheets of paper] in active files.

He estimated about 17 percent of those files would be classified, then conceded: "Based upon the collective judgement here, I would think, including reproduced copies, there could be more than 20 million classified documents."

However, in later hearings, Cooke put the numbers in proper prospective by noting the "volume of classified material constitutes less than 5 percent of the total official records created by the Department."[4]

Congressman Reid sought to comprehend the volume of paper being discussed. His staff determined DOD classified paper "equals 18 stacks of documents 555 feet

---

[3]U.S., Congress, House, U.S. Government Information Policies and Practices (Part 2), op. cit., p. 658.

[4]U.S., Congress, House, Committee on Government Operations, Security Classification Reform, Hearings Before a Subcommittee on H.R. 12004, 93rd Cong., 2d Sess., 1974, p. 75.

high, each as high as the Washington Monument."[5]

One State Department witness testified his department had approximately 35 million classified documents in its possession. Another State Department representative estimated the total to be only 2 million.[6] The agencies were at a loss to competently describe the enormous volume of classified information.

The most definitive estimate was presented by Dr. James B. Rhoads, Archivist of the United States.

> We have in our custody approximately 30 billion pages of Federal records, something more than 40 percent of the total volume of the Government's records ....
>
> We estimate that for the period 1939 through 1945 the National Archives and the several relevant Presidential Libraries possess approximately 172 million pages of classified material ....
>
> For the period 1946-50 we estimate our classified holding at approximately 150 million pages, and for the period 1950-54 we estimate an additional 148 million pages. These estimates indicate that for the period from the beginning of the Second World War through the end of the Korean War we possess some 470 million pages of classified documents.[7]

---

[5]U.S., Congress, House, U.S. Government Information Policies and Practices (Part 2), op. cit., p. 685.

[6]Dorsen and Gillers, p. 72.

[7]Part 7, p. 2605.

Rhoads went on to say that the total volume of classified documents is much greater, of course, because relatively few documents originated later than 1954 repose in the National Archives. That almost half a billion pages represents but a fractional part of the total classified volume in existence. The problem is compounded by unknown numbers of reproduced copies.[8]

Finally, the Interagency Classification Review Committee (ICRC) found declassifiers unable to compete with classifiers when it reported more than 4.5 million "classification actions" occurred in 1976. During 1973 through 1975, about 4 million documents were originally classified annually.[9]

## Derivative Classification

Executive Order 11652 sought to classify less and declassify it faster. To meet the first task, the drafters wanted fewer classifying agencies and individuals;

---

[8]For a discussion of the volume of classified information and the effectiveness of E.O. 11652, see Archivist James Rhoads' statement: U.S., Congress, House, Security Classification Reform, op. cit., pp. 50-4.

[9]ICRC, 1976 Progress Report, op. cit., p. 20.

both were drastically reduced.[10]

Under Executive Order 10501, as amended, 46 executive entities had classification authority.[11] In 34 of these, the authority could be delegated by departmental or agency head. A government information subcommittee August 1971 questionnaire discovered about 55,000 government officials in 12 selected agencies authorized to classify information.[12] The Department of Defense was high scorer with 29,837. (At the end of 1976, authorized classifiers totalled 13,976.[13]) These statistics don't account for the extent of "derivative classification," the clerical reassignment or transfer of an existing classification when portions of one classified document are used in another document.[14]

William Florence described the evils inherent in derivative classification during hearings in 1971.[15]

---

[10] Barker, p. 20.

[11] E.O. 10501, 3 CFR, 1949-53 Comp., op. cit., sec. 2 (a) (b).

[12] Part 7, pp. 2929-37.

[13] ICRC, 1976 Progress Report, op. cit., p. 10.

[14] H. Rept. 93-221, p. 39.

[15] Part 1, pp. 98 and 104.

> ... A DOD regulation delegates something called derivative classification authority to any individual who can sign a document or who is in charge of doing something.
>
> Such individual may assign a classification to the information involved if he believes it to be so much as closely related to some other information that bears a classification.
>
> In the past several years I have not heard one person in the Department of Defense say that he had no authority to classify information.
>
> * * * * * * * * * * * *
>
> Under this concept of derivative authority to classify, anyone can assign classifications.... I used the statement, I believe, "hundreds of thousands" in my comments.

The State Department readily acknowledged the existence of derivative classification when it explained the classification of a new document containing previously classified parts "... derives from the earlier classified source, and is simply an acknowledgment of an authorized classification action already taken. We have no measure of the proportion of such classification in this department, but do not believe it to be great."[16]

A document is classified at the highest level afforded information therein. Therefore, a frightfully large number of documents may be highly classified because

---

[16] Part 7, p. 2517.

of the derivative classification practice.[17] The State Department is one of the few which requires all classification be made by an official with original classification authority.

Additional questions submitted by the House subcommittee to J. Fred Buzhardt, DOD general counsel, yielded a more reluctant admission of derivative classification existence. Buzhardt said the practice was given official life under E.O. 10501 by DOD instruction 5210.47 but the current DOD directive (5200.1-R, Nov. 1973) omitted reference to the term. Nor could he provide the volume of information or number of persons involved in the practice. Under E.O. 11652, Buzhardt said, "It is expected that the total volume of information to which classification markings will be applied pursuant to classification guidance will be substantially less than in the past...."[18]

The term was excised from DOD regulations but not the practice. Two years later (1974), David O. Cooke, assistant DOD secretary, admitted the existence and necessity of continued derivative classification. A

---

[17] Ibid., p. 2523.

[18] Ibid.

paragraph of the most recent DOD information security regulation, 5200.1-R, allows classification of information determined to be "in substance the same as" already classified information. Cooke rather torturously explained that an original classifier and one who marks a document containing information substantially the same as already originally classified information are really one administrative entity.[19]

> It is not intended that those who lack original classification authority have a right to classify information not known to be already classified. However, what is intended is that persons not having original classification authority are obligated to afford the same *degree of protection* to information which is originally classified by an authorized official. In these cases, the person without original classification authority is not making a fresh judgment as to whether the information which he is dealing with is in substance the same as that which is already classified.

Despite DOD's semantic play, the ICRC, responsible for overseeing implementation of E.O. 11652, recognized derivative classification in their report for 1976:[20]

> It is the considered opinion of experienced security officials that the vast majority of material which is classified in the executive

---

[19] U.S., Congress, Senate, Government Secrecy, op. cit., p. 248.

[20] ICRC, 1976 Progress Report, op. cit., p. 30.

> branch is so marked based on the classification of a source document, written classification guides, or other forms of classification guidance .... To prohibit the application of derivative markings would greatly impede the orderly flow of administration, particularly in the larger Departments with their dispersed locations. Further, any such drastic action would, of necessity, require a significant increase in the number of original classifiers. (Emphasis added.)

This recognition seems to negate what was lauded as one of the most salutary results of the Nixon order---a reduced number of classifiers.[21] And the concept of specified personal accountability receives an almost mortal blow. However, widespread usage of paragraph markings (authorized by DOD in 1964) and reliance on classification guides issued by original classifiers does tend to curtail the indiscriminate classification under previous orders.[22]

The numbers of original classification authorities did take a drastic cut, and continue to decline under the current order. The total number of original classifiers dropped from 59,316 under E.O. 10501 to 13,976, a 76 percent decline. Such classifiers in DOD dropped an

---

[21] U.S., Congress, Senate, Executive Privilege, Vol. III, op. cit., p. 608.

[22] See: H. Rept. 93-221, chapter 5.

astounding 86 percent, from 30,542 to 4,265.[23]

After a valiant beginning, the 1976 ICRC report shows the bureaucracy may be asserting itself again. In 1976 the number of original classifiers continued to decline but the number of classification actions increased by about three-quarters of a million.[24] The report could not give a specific reason for the increase.

While the number of original classifiers has declined, the number of departments and agencies given classification authority has slowly increased from 23 in 1972 (including executive office agencies) to 40 in 1976.[25] That is but seven fewer than allowed under E.O. 10501. President Jimmy Carter added in June 1977 to the list of authorized classifying agencies.[26] The order gives the top three individuals in the Office of Drug Abuse Policy original Top Secret classification authority.

## Overclassification

Supreme Court Justice Stewart eloquently struck

---

[23]ICRC, 1976 Progress Report, op. cit., p. 10.

[24]Ibid., p. 14. [25]Ibid., p. 10.

[26]U.S., President, "Classification of National Security Information," Federal Register 42, 27 June 1977, 33257.

to the very heart of the overclassification problem.[27]

> I should suppose that moral, political, and practical considerations would dictate that a very first principle of that wisdom would be on insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hall-mark of all truly effective internal security systems would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.

If bureaucrats could internalize and abide by those thoughts, there would be no need for the reams of regulations governing the executive secrecy system.

Four years after the Pentagon Papers case, the Wall Street Journal reiterated the problem of overclassification without flourish. "Mile after mile, acre after acre, in metal cabinets and on computer tapes, the confidential files of Uncle Sam grow steadily and, some say ominously. Who knows what they contain?"[28]

One example of overzealous classification surfaced through the Army's "Project Declassify" begun in 1969

---

[27] New York Times v. U.S., 403 US 713 at 729, Justices Stewart and White, concurring.

[28] Wall Street Journal, 27 June 1975, p. 1.

which used reservists to declassify 60 million pages of Army secrets dating back to 1913. The Army released a previously "restricted" 1939 photograph which revealed a secret German pre-World War II invention. This diabolical war-machine could now be revealed officially for the first time. It was a Volkswagen.[29]

Speaking at an Associated Press luncheon in New York on April 20, 1970, Defense Secretary Melvin Laird recognized the overclassification problem:[30]

> Let me emphasize my convictions that the American people have a right to know even more than has been available in the past about matters which affect their safety and security. There has been too much classification in this country.

Classification expert Florence testified to the House subcommittee in 1971:[31]

> I sincerely believe that less than one-half of 1 percent of the different documents which bear currently assigned classification markings

---

[29] "Army Reveals Long-Classified Secrets," FoI Digest 18 (March/April 1976):6.

[30] U.S., Congress, House, Committee on Government Operations, Hearings, U.S. Government Information Policies and Practices--The Pentagon Papers (Part 3), 92d Cong., 1st Sess., 1971, p. 975.

[31] Part 1, p. 97.

> actually contain information qualifying even for the lowest defense classification under Executive Order 10501. In other words, the disclosure of information in at least 99½ percent of those classified documents could not be prejudicial to the defense interests of the Nation.

Former United Nations Ambassador and Supreme Court Justice Arthur Goldberg was slightly less disbelieving of the propriety of classifications.[32]

> I have read and prepared countless thousands of classified documents. In my experience 75 percent of these documents should never have been classified in the first place; another 15 percent quickly outlived the need for secrecy; and only about 10 percent genuinely required restricted access over any significant period of time.

The simplicity of overclassification was stated in 1972 by Gene R. LaRocque, Rear Admiral (retired), a much-decorated veteran of 31 years of naval service.[33]

> Regrettably, far too much material is classified, much of it just because it is easier to classify than not .... And, it is easier to maintain secure files if all material is classified. In that way, only one set of files need be maintained.
>
> Classification is also very simple; all one needs is a typewriter or a Secret stamp. In most offices, the secretaries or the yeomen establish the classification ....

Senator Jacob Javits revealed what everyone

---

[32] Ibid., p. 12.

[33] Part 7, pp. 2909-10.

instinctively knew to be true in a remark during a 1976 floor debate. "It is not providence on Mount Sinai that stamps a document Secret or Top Secret but a lot of boys and girls just like us who have all their own hang-ups."[34]

Executive Order 11652 did not solve the over-classification problem.[35] When the flow on information to the outside is limited, it also becomes limited within. The House Select Committee on Intelligence found National Security Agency reports of the impending outbreak of the 1973 Middle East war had been considered too "sensitive" to be shown to a key military analyst. That meant there was no way for him to predict the war's beginning.[36]

Theodore C. Sorensen, President Carter's first nominee for CIA Director, submitted an affidavit on behalf of Anthony Russo, Jr., and Daniel Ellsberg at the 1973 district court trial.[37] Sorensen recognized the need for

---

[34]Martin Michaelson, "Up Against the Stone Wall," The Nation 224 (21 May 1977):617.

[35]For a few examples, see: U.S., Congress, House, Security Classification Reform, op. cit., pp. 70, 497, 262-3.

[36]Christine M. Marwick, "Reforming the Intelligence Agencies," First Principles 1 (March 1976):5.

[37]U.S. v. Anthony Joseph Russo, Jr. and Daniel Ellsberg, No. 9373 - (WMB) - CD, District Court - Central District California (1973).

a limited amount of government secrecy but said:[38]

> I can flatly state that Top Secret stamps are frequently and routinely applied with only the briefest and loosest consideration of what, if any, direct and concrete injury to the nation's security interest would result if the general public were to be granted access to the information ....

In the 1970's, as various theoreticians attempt to explain the cause of the overclassification phenomenon, three different theories arise. One is that people stamp things at a higher classification than they should because they want to cover up mistakes.[39] The second reason has to do with the idea of maintaining power.[40] If people

---

[38]U.S., Congress, Senate, Select Committee on Intelligence, Nomination of Theodore C. Sorensen, Hearings, 95th Cong., 1st Sess., 1977, p. 18.

[39]Jeanni Atkins and Belvel J. Boyd, "Classification Reexamined," Freedom of Information Center Report No. 332 (Columbia, MO: Freedom of Information Center, 1976), p. 3; U.S., Congress, Senate, Committee on the Judiciary, Congressional Access to and Control and Release of Sensitive Government Information, Hearings Before the Subcommittee on Separation of Powers, 94th Cong., 2d Sess., 1976, p. 14; Ben H. Bagdikian, "What did we learn?" Columbia Journalism Review 10 (September/October 1971): 48.

[40]U.S., Congress, Senate, Congressional Access, op. cit., p. 15; Barker, p. 4.

don't know what is happening they can't question or challenge government action. The third reason is common, as Admiral LaRocque testified in 1972.[41] It is just following the easiest path through the bureaucratic tangle; keep the information secret because it is easier that way.[42] Human pressures on the person with the classification stamp dictate some acquiescence to rule bending. Press critic Ben Bagdikian said that somehow the burden has shifted from government having to prove why it should conceal information, to the citizen, who has to prove why he should be told.[43]

Tom Wicker, New York Times columnist, in 1971 related a conversation he had with a high government official.[44] The official classified everything going through his office Top Secret, not on the rationale that was the way to get other officials to read it, but because in the entire time he had been in government nobody had given him really rational reasons for classifying a document or not.

---

[41] Part 7, pp. 2909-10. [42] Birmingham, p. 27.

[43] Bagdikian, p. 49.

[44] "Where We Stand," Columbia Journalism Review 10 (September/October 1971):27.

The overburdened executive often unwittingly promotes overclassification.[45] Busy managers may ask to see only higher classified traffic and subordinates eager to pique their supervisor's interest will classify papers Top Secret. For example, an intelligence agency sponsored a conference in Washington in 1975 where attendees received a brochure classified Top Secret with a special codeword caveat. The brochure contained classified lists and subjects to be discussed. The host admitted the brochure contained no classified information but explained the classification was necessary "to get anything coordinated in this building."[46]

Security expert William Florence enumerates eight reasons most commonly used by individuals for classifying information. These reasons have nothing to do with national security interests or concerns. Florence's list includes:[47]

---

[45] Birmingham, pp. 27-8. [46] Ibid., p. 28.

[47] U.S., Congress, Senate, Committee on Government Operations and the Subcommittee on Separation of Powers and Administrative Practice and Procedure of the Committee of the Judiciary, Executive Privilege, Secrecy in Government, Freedom of Information, Hearings Before the Subcommittee on Intergovernmental Relations on S. 858, S. Con. Res. 30, S.J. Res. 72, S. 1106, S. 1142, S. 1520,

> (1) newness of information; (2) keeping it from newspapers; (3) foreigners might be interested; (4) don't give it away--and you hear the old cliche, don't give it to them on a silver platter; (5) association of separate nonclassified items; (6) reuse of old information without declassification; (7) personal prestige; and (8) habitual practice, including clerical routine.

Simple overclassification of true national security material is compounded by the classification of unclassified information. Just the idea seems incongruous in the context of E.O. 11652's avowed purpose of reducing classification. In 1971, Florence described a Navy practice of classifying newspaper items, now discontinued.[48]

DOD regulations recognize and allow classification of unclassified information.[49]

> The general rule is that a compilation of unclassified items shall not be classified. In rare and unusual circumstances, however, a classification may be required if the combination of unclassified items together provides an added factor which warrants classification.

Author and former newspaperman, David Wise, describes in his book, The Politics of Lying, government

---

S. 1923, S. 2073. Vol. I, 93rd Cong., 1st Sess., 1973, p. 287.

[48] Part 1, p. 100.

[49] 32 CFR 159 at sec. 202-14, July 1976.

manipulation of classification procedures to conceal the fact satellites are effectively used to police arms control agreements. At the request of the Defense Department, the Arms Control and Disarmament Agency made an unclassified study of satellite surveillance technology in 1965. The unclassified report said satellites were capable of monitoring an arms agreement. However, the study was graded Top Secret and no copies were ever published.[50]

William Florence provided another example in May 1972 testimony to the House government information subcommittee. An Air Force manual entitled "Assembly Manual--Gyro Float" was issued February 1971 with the classification Confidential. The document contained the following statement:[51]

> Each section of this volume is in itself unclassified. To protect the compilation of information contained in the complete volume, the complete volume is Confidential.

Florence maintains unclassified plus unclassified never

---

[50] McCartney, "What Should be Secret," op. cit., p. 42.

[51] Part 7, p. 2534.

equals classified. If information is unclassified, it should always be so.

Assistant Defense Secretary Cooke was asked by the Senate to explain the procedure in 1974. Cooke said DOD regulation 5200.1-R delineated factors to be carefully considered prior to issuing a classification. Cooke continued:[52]

> It is not the intention of the Department ... that information be indiscriminately classified because it could be associated with other information already in the public domain ....
>
> Under no circumstance will an item which has been officially released to the public be classified.

The whole document may carry a classification, thus effectively hiding the unclassified item from public view even though paragraphs applicable to it are marked "Unclassified."

The examples of overclassification provided above range from the ridiculous to the understandable. However, in the area of science, overclassification can threaten our very survival.

Dr. Donald J. Hughes, former president of the

---

[52]U.S., Congress, Senate, Government Secrecy op. cit., p. 249.

American Federation of Scientists, appeared before the subcommittee on government operations in 1958 and said:[53]

> Because of intimate relationships of the many branches of basic research to each other, it is vital scientists have ready access to a great range of technical literature with minimum delay. Because of the importance of research to later military developments, the flow of information, which is vital to development of basic science, has direct bearing on the actual survival of our nation.

Dr. Earl Callen, professor of physics at American University, restated the basic view against scientific secrecy before a Senate subcommittee in 1973. "Secrecy is inimical to science. Science flourishes best in an atmosphere of free and open inquiry."[54]

Nuclear physicist Dr. Edward Teller believes scientific discovery is based upon basic laws of nature and cannot be kept secret more than a year.[55] Teller points to the stifling effects of secrecy during the days of alchemy. Though a great deal of good scientific work

---

[53] Birmingham, p. 23.

[54] U.S., Congress, Senate, Executive Privilege, op. cit., p. 302.

[55] See Dr. Teller's Statement in: U.S., Congress, Senate, Government Secrecy, op. cit., pp. 253-7 and 258.

was performed by alchemists, it bore little fruit because secrecy prevented the type of collaboration essential to scientific growth. Despite the shroud of secrecy thrown over nuclear development, the United States was not long the only country with nuclear weapons. On the other hand, a more open policy permitted rapid development of electronic computers, a field in which the U.S. maintains undisputed leadership.

According to Teller, this penchant for scientific secrecy is actually provocatively dangerous.[56]

> Our policy of secrecy in science and technology has created the illusion that we are in possession of valuable information which is not available to other nations, and in particular, not available to our chief competitor, the Soviet Union .... Secrecy in the nuclear field has also the opposite result of raising fears of the unknown.

In 1970 the Pentagon asked its Defense Science Board to study and make recommendations on defense secrecy.[57] The Board found it unlikely that "tightly controlled" information would stay secure as long as five years. Truly "vital" information would be compromised within a year. The task force said, "Classification may

---

[56] Ibid., p. 253.

[57] *U.S., Congress, House,* Security Classification Reform, op. cit., pp. 623-42.

sometimes be more effective in withholding information from our friends than from our potential enemies."[58] The amount of scientific and technical information which is classified could be reduced as much as 90 percent. And because of secrecy, "the laboratories in which highly classified work is carried out have been encountering more and more difficulty in recruiting the most brilliant and capable minds.[59] The Board felt the overburdening belief in the need for secrecy could lead to mediocre weapons research. Ironically, in our attempt to preserve our superior technological position, we are in fact endangering that position.

It appears, then, that overclassification exists and no mere alteration in executive orders, rule and regulations will magically cure the situation. That's why continued education of the system's users remains paramount. The valiant struggles do not always overcome acquiescence. At his 1977 nomination hearing, Ted Sorensen said:[60]

> What it all boils down to is this: The government has always recognized and accepted

---

[58] Ibid., p. 633. [59] Ibid., p. 641.

[60] U.S., Congress, Senate, Nomination of T.C. Sorensen, op. cit., p. 25.

> the fact that arbitrary, inconsistent and indiscriminate overclassification of documents exists; and that consequently large amounts of classified material are passed from the government to the public --- sometimes to the government's embarrassment, occasionally even to its injury --- as a part of the system of governing and living in an open society.

Sorensen's comment implicitly recognizes the widespread practice of selective release of classified information leaks. Full consideration of the topic lies outside the scope of this paper.[61] However, the practice of leaking information, for good or ill reasons, results from garantuan overclassification. Government administrators must leak information for the government to function, for programs to receive support. Max Frankel, former New York Times Washington bureau chief, described in 1971 the government's employment of classified information.[62]

> Its purpose is not to amuse or flatter a reporter whom many may have come to trust, but variously to impress him with their stewardship of the country, to solicit specific publicity, to push

---

[61] For a good summary see: "Leaks: Concern and Control," Freedom of Information Center No. 356 (Columbia, MO.: Freedom of Information Center, 1976).

[62] Max Frankel, "The 'State Secrets' Myth," Columbia Journalism Review 10 (September/October, 1971): 23. Also see: Statement by Arthur Schlesinger, Jr., U.S., Congress, House, Security Classification Reform, op. cit., pp. 494-504; Barker, p. 16.

> out diplomatically useful information without official responsibility ....

## Industrial Security Program

The contagion of the classification philosophy is not contained within government but spread throughout industry and academe. The industrial security program adds a whole new element and set of regulations to the classification system. More than 11,000 industrial facilities and academic research centers are cleared by DOD to handle and have custody of classified information.[63]

Industries with defense contracts received a 16½-page Department of Defense Industrial Security Manual in 1951. The manual is now 272 pages of detailed security instructions. The Federal Register published in 1955 a DOD directive which advised defense contractors to avoid publishing information that was of "possible use to a potential enemy."[64] This definition went beyond even the bounds of a damage to national security test and the Associated Press Managing Editors Association condemned

---

[63] Cox, p. 75.

[64] Wiggins, p. 110, and 15 September 1955 Federal Register.

the actions when they adopted a resolution stating:[65]

> The association expressly condemns the withholding of information that has not been classified and that is not eligible for classifying on the excuse that even though it is nonsecurity information it might be of "possible use" to a potential enemy.

The current program's genesis is Executive Order 10865, issued by President Eisenhower on February 20, 1960. The order authorizes industrial personnel security clearances and gives DOD responsibility for administration of classified contracts. The program is essentially

> a Government/industry team program, wherein the Government establishes requirements for the protection of classified information entrusted to industry and industry implements these requirements with Government advice, assistance, and monitorship.[66]

Maj. Gen. J.J. Cody outlined the program's operation in a 1974 statement to the House government information subcommittee.[67] An organization doing DOD classified contract work must first receive a facility security clearance, meaning the operation is certified not a

---

[65] Wiggins, p. 110.

[66] U.S., Congress, House, Security Classification Reform, op. cit., p. 142.

[67] Ibid., pp. 142-63.

communist front or some other poor security risk. The organization is required to sign a security agreement.[68] Under the agreement's terms, the private facility must adhere to all government rules for safeguarding classified information. The House government information subcommittee found this costs a lot of money.[69] The industries and universities that have the armed guards, secure storage and burn facilities don't protest because the government pays almost all expenses.

Once cleared, a contractor strives to maintain that status. The business can't get many DOD contracts nor stay abreast of recent technological developments without that clearance. Therefore, pressure is great not to question the workings of the security system. The firm's security officer assumes a key administrative position. Employees must receive security clearances (more on this later). Despite a person's academic credentials, if there

---

[68] The Agreement's specifications are guided by DOD regulation 5220.20-R, "DOD Industrial Security Regulation.

[69] H. Rept. 93-221, pp. 49-51 and William G. Florence, "Executive Secrecy: Two Perspectives," Freedom of Information Center Report No. 336 (Columbia, MO.: Freedom of Information Center, 1975), p. 2.

is the slightest doubt about his trustworthiness, the firm may feel compelled not to hire him.[70]

The Pentagon found that contractors try to maintain their cleared status. A 1974 Pentagon inspection of 14,000 cleared facilities showed almost half had no classified material.[71] The inspection revealed 1,357 facilities with custody of less than five items of classified material.[72] A 1972 inspection had produced similar results.[73] The rewards accorded receipt of a DOD contract are so great, industries are willing to maintain expensive facilities to stay on the 'cleared' list.

However, contractors have no authority to determine original classification.[74] Classification guidelines are provided by contracting agencies but any classification is subject to review and certification by an agency

---

[70]See: U.S., Congress, House, Security Classification Reform, op. cit., pp. 420-32; U.S., Congress, Executive Privilege, Vol. 1, op. cit., pp. 305-7.

[71]Cox, p. 78.

[72]U.S., Congress, House, Security Classification Reform, op. cit., p. 253.

[73]U.S., Congress, Senate, Government Secrecy, op. cit., p. 235.

[74]U.S., Congress, House, Security Classification Reform, op. cit., p. 148.

classification management specialist. This puts the classification manager on the spot. He is personally responsible for the classifications stamped on material leaving his facility but probably is not physically able to do more than concur with previously affixed classifications, particularly in large projects.

What impact did E.O. 11652 have on these private firms and institutions? Did the order accomplish its task of reducing classified information? In 1973 William Florence said:[75]

> One research corporation under contract to DOD stated ... the only effect E.O. 11652 had on its classified work was the expenditure of over $4,000 for rubber stamps to reflect new notations such as the exemption of information from automatic declassification.

Florence verified that statement by personally visiting companies which held more than 2500 classified contracts valued at $1.2 billion.[76] He found the working level bureaucracy had resisted deemphasis of classification.

---

[75] U.S., Congress, Senate, Executive Privilege, Vol. 1, op. cit., p. 287.

[76] U.S., Congress, 20 December 1974, Congressional Record 120:42020.

## Access and Distribution

A common thread runs through the fabric of access to classified information. Whether a person is a scientist, private technician or a government employee, if he wants to taste of the honeydew of secrecy he must have a security clearance, as Section (6) (a) of E.O. 11652 states:

> No person shall be given access to classified information or material unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of his duties.

Without such clearance, the employee is locked out of his job. Obviously, this results in a powerful method of bureaucratic control. The concern of the system is whether or not an applicant will not rock the boat. The security system could be used to make sure he won't.

The clearance procedure was described in 1972 by Joseph Liebling, DOD assistant secretary, and includes a national agency check, background investigation or both, depending upon sensitivity of the information with which the person will work.[77] The more extensive background investigation extends 15 years into a person's past or

---

[77] U.S., Congress, House, Hearings on the Proper Classification, op. cit., pp. 17419-23.

to his eighteenth birthday. The record is updated every five years. Despite the lengthy and costly procedures, a clearance is not inordinately difficult to acquire. In 1971 government-granted security clearance just for civilian contractors numbered almost one million.[78] In the past twenty years more than five million citizens have been cleared.[79]

Section (6) (a) specified also the second requirement for access to classified information --- a need to know. This portion of the access to classified information dichotomy gives rise to the phenomenon of access and distribution markings. As far as the general public is concerned, but three classifications exist --- Top Secret, Secret and Confidential. However, voluminous internal governmental notations restrict dissemination further than implied by the 3-tiered classification system.

The "distribution controls" are based upon Section 9 of E.O. 11652.

> 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 materials, including

---

[78] Ibid., p. 17421. [79] Cox, p. 76.

those which presently relate to communications, intelligence, intelligence sources and methods and cryptology.

The rationale behind use of such markings and the confusion they produce is illustrated by two colloquies during 1972 Congressional hearings.[80]

> Mr. Moorhead. Mr. Blair, in responding to the subcommittee's questionnaire the [State] Department listed several authorized "channel captions." How do these authorized channel captions control information? What authority is there for the use and do they really in effect serve as classification devices?
>
> Mr. Blair. Well they are not classification devices, Mr. Chairman, they are internal government distribution controls which attempt to enforce the need-to-know principle .... So far as availability of the document to the public is concerned, it has no bearing whatsoever. The classification, of course, would govern.

The Defense Department General Counsel, J. Fred Buzhardt, was similarly questioned.[81]

> ... We are talking about two entirely different things. If we start with classified documents, those documents are not to be revealed to unauthorized persons.
>
> ... Once the determination is made that information must be protected, one of the devices used to protect it is not to disseminate it beyond those who have some official reason or a business reason to use the information....
>
> As a consequence, access limitations are imposed, sometimes by marking on the document,

---

[80] Part 7, p. 2477. [81] Ibid., p. 2479.

> sometimes because the man doesn't show it to his subordinates, for instance, he makes a judgment they do not need to see it.

The wording in the current DOD classification regulation leaves some doubt as to the possible extralegal nature of access control markings. The regulation defines special access programs as "... any program imposing a 'need-to-know' or access controls beyond those normally provided for access to Confidential, Secret or Top Secret information."[82] (Emphasis added.)

The use of access markings is not a new practice. Former Secretary of Defense McNamara found himself in a ticklish situation in 1964. Testifying before the Senate Foreign Relations Committee, McNamara hesitated to explain the source of a report that North Vietnamese patrol boats were about to attack the Turner Joy. The following conversation resulted:[83]

> The Chairman [W. Fulbright]: ... He is talking of a special classification of intelligence communications....
>
> Senator Gore: Mr. Chairman, could we know what particular classification that is? I had not heard of this particular super classification.

---

[82] 32 CFR, sec. 159.1200-1 (a).

[83] Wise, p. 59.

> Secretary McNamara: ... Clearance is above Top Secret for the particular information involved in this situation. (Emphasis added.)

While the semantics in the current DOD regulation are different than in 1964 and there is a clear rationale for use of access or control markings, the basic problem is the effect their proliferated use has on effective operation of the classification system. Their very existence partially proves the reality of overclassification. Special designations are needed to identify what is really secret. The Congressional Research Service found more than just a few access and control labels in use in 1972. The Service found 63 such labels.[84]

During the 1972 government information subcommittee hearings, William D. Blair, Jr., deputy assistant secretary of state for public affairs, attempted to explain distribution and access markings. Blair said,

> "Limited official use" is not a fixed distribution channel, such as some of these other terms you have mentioned. It is simply an administrative red flag put on that document which means that the document should be given the same degree of protection, physical protection as a classified document when though it is not, under executive

---

[84] Part 7, p. 2493, and pp. 2734-5 for a list of State Department control captions.

order, classifiable.[85]

Subcommittee staff member William H. Copenhaver was apparently unconvinced that another level of classification was not being used and said:[86]

> May I say, to conclude, that all you have convinced me of is to reinforce my belief that a distribution marking is merely a more restrictive or stricter type of classification marking.

The Interagency Classification Review Committee (ICRC) recognizes the difficulty posed by such markings. The committee says the terms have no generally understood meaning outside the originating department and, therefore, confuse an outside recipient "with respect to the handling of and extracting from the document. Further, the use of such terms implies the existence of security classification categories than those prescribed in the Order."[87]

Closely related to the problem of access markings is the practice of affixing restrictive markings to documents that don't contain classified information. DOD General Counsel Buzhardt was asked during hearings to explain "For Official Use Only."

---

[85] Part 7, p. 2478. [86] Ibid., p. 2479.

[87] ICRC, 1976 Progress Report, op. cit., p. 30.

> Mr. Buzhardt. Mr. Chairman, that is not a security classification. For Official Use Only means that it is not for public disclosure.
> Mr. Nedzi. Under penalty of What?
> Mr. Buzhardt. There are no penalties for that. There are things which are not classified, which are not releasable.[88]

Some of these markings are similar to authorized classifications: "(Agency) Confidential" and "Conference Confidential."[89] The ICRC discovered the markings were applied to designate information which may be permissively withheld from public release under the Freedom of Information Act. Nonetheless, the markings cause confusion, proliferate improperly classified information and degrade the classification system.

The ICRC's solution? The chairman sent a strong letter to Departmental senior officials.[90] Staff member visits during 1976 discovered use of unauthorized markings was decreasing.

## Costs

Security is not cheap. Maintenance of the classification system is costly in terms of dollars as well as

---

[88] U.S., Congress, House, Hearings on the Proper Classification, op. cit., p. 17441.

[89] ICRC, 1976 Progress Report, p. 30. [90] Ibid.

damage to the American psyche. The loss of public trust and support in and for government is more injurious than squandered dollars.[91] The protection of information essential to the safety of the nation requires information carrying a classification mark be truly significant.

In 1972, Alaskan Senator Mike Gravel said:[92]

> I think the cocoon of secrecy that we have woven over the years, particularly since the Second World War, is what has permitted us to go into Vietnam, permitted us to waste not only our blood, our young people, but also to waste our economic fiber. To what degree I don't think we will ever know. I think only history can judge that.
>
> I personally feel that our democracy is under assault, assault in a very unique way and in a very evolutionary way, and unless we can turn the tide we will lose the system of government we presently enjoy. And the single item that will be responsible for this loss of government ... will be secrecy itself and nothing more, nothing more complex than that, because secrecy is anathema to democracy. It is that fundamental.

That same year Congressman William Moorhead, less passionately, but no less to the point, said:[93]

> How can our government maintain our own national security and the confidence of our

---

[91] Birmingham, p. 23. [92] Part 7, p. 2553.

[93] Thomas M. Franck and Edward Weisband, editors, Secrecy and Foreign Policy (New York: Oxford University Press, 1974), p. 89.

> global partners if its system of classification lacks integrity, is administratively unworkable, and is abused by overclassification to the point where patriotic Americans feel compelled to leak or otherwise compromise such information.

If concern for a devalued ideal does not pique the reader's interest, the actual dollar cost will. One difficulty in totalling up dollars spent on the classification system results from the many and far-flung facets of the system. Costs must include expenditures for clearances, the classification activity itself, handling and storing classified material, physical security, administration, destruction and declassification.[94]

The Defense Department said in 1971 it had "no available data on the total costs which could be attributed to security classification or to the protection and handling of classified documents and material."[95] But in 1972 William Florence testified:[96]

> Last year, I estimate that about $50 million was being spent on protective measures for classified documents which were unnecessarily

---

[94] Part 7, p. 2286.

[95] U.S., Congress, House, Hearings, The Pentagon Papers (Part 2), op. cit., pp. 690-1.

[96] Part 7, p. 2532.

> classified. After further observation and inquiry, and including expenditures for the useless clearances granted people for access to classified material, it is my calculation that the annual wastage for safeguarding documents and equipment with counterfeit classification markings is over $100 million.

A June 1971 General Accounting Office (GAO) study commissioned by the House subcommittee provided a more precise estimate. The completed study of four selected agencies --- Defense, State, Atomic Energy Commission and National Aeronautics and Space Administration --- appeared in the Congressional Record.[97] Direct costs for the four agencies totaled $60.2 million. This figure does not include an additional $66.1 million spent for personnel security investigation.

That $60.2 million estimate is only a fraction of total costs within those four agencies because security costs associated with Government classified contracts are not identified separately. These costs are "overhead."[98] In responding to the GAO, the Defense Department conducted a limited survey which determined 0.7 percent of contract

---

[97] 15 May 1972, also see Part 7, pp. 2286-93.

[98] H. Rept. 93-221, p. 50.

price was attributed to security costs.[99] If that percent estimate is applied to DOD's research budget for fiscal 1970, as much as $49 million could be added to DOD security costs.[100]

The security costs incurred by one specific contractor illustrates the common problem. Albert H. Becker, research security coordinator for Georgia Institute of Technology, testified before the House subcommittee in 1974. Becker estimated it cost Georgia Tech $58,000 a year "to meet the security requirements over the last ten years."[101] Becker said the change in the security system necessitated by Nixon's executive order cost his institution $8,000.

Still other costs are not included in the GAO estimate.[102] Three of the four agencies did not provide estimates for administration and enforcement of security policies, procedures and regulations. The State Department

---

[99] Part 7, p. 2290.

[100] H. Rept. 93-221, p. 51.

[101] U.S., Congress, House, Security Classification Reform, op. cit., p. 431.

[102] Part 7, p. 2287.

did not estimate cost for declassification activities.

The National Archives found that declassification is expensive, though not as costly as the continuing classification system. The National Archives is primarily involved in reviewing and declassifying records more than 30 years old.[103] In 1975 it reviewed 63 million pages, declassifying better than 99 percent of them. Testifying for a 1977 budget request, before a House appropriations subcommittee, Archivist Rhoads asked for $1,410,000 to maintain a staff of 105 persons involved in declassifying documents.[104]

This section spotlighted some of the major problems hindering efficient operation of the security classification system. Above all the administrative manipulations, the weakest link remains the human being entrusted with making the system go. But the troubles continue --- overclassification breeds unending volume which consumes extravagant amounts of money. How to contain the excesses, the leaks?

---

[103] E.O. 11652, sec. 5 (E) (1).

[104] U.S., Congress, House, Committee on Appropriations, Treasury, Postal Service, and General Government Appropriations for Fiscal Year 1977, Hearings Before a Subcommittee, Part 5, 94th Cong., 2d Sess., 1976, pp. 191-6.

Chapter VI discusses sanctions against violators of the system.

# CHAPTER VI

## SANCTIONS

The grand hope after 1972 that Executive Order 11652 would successfully modify the security classification system to produce fewer official secrets and more information for the public bore little fruit. The order holds each classifying authority accountable for the propriety of classifications attributed to him.[1] That person's name is supposed to be displayed on the front of all such documents. The system is not even that rigid.[2]

Various departments, notably DOD, are allowed to use code designations or a notation of the document's originating location and organization or source document or classification guide.[3] The National Security Council's

---

[1] E.O. 11652, sec. 4 (B) and NSC Directive I (C).

[2] ICRC, Progress Report, 31 March 1973, pp. 3-4; 1976 Progress Report, p. 30.

[3] E.O. 11652, sec. 4 (B) and H. Rept. 93-221, p. 69. See an Atomic Energy Classification Guide in U.S., Congress, House, Security Classification Reform, op. cit., p. 505.

implementing directive calls for doubts to be resolved in favor of disclosure.[4] The intent of the directive alone does not overcome the inherent reluctance of a classifier to err on the side of disclosure. That natural reluctance is bolstered by the more austere punishment awaiting under-classifiers.

The current order warns "both unnecessary classification and overclassification shall be avoided."[5] An overclassifier will be

> notified that his actions are in violation of the terms of this order or a directive of the President issued through the National Security Council. Repeated abuse of classification process shall be grounds for an administrative reprimand.[6]

Underclassifiers fare worse. Section 13 (B) says:

> The head of each Department is directed to take prompt and stringent administrative action against any officer or employee of the United States... determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by or under this order or a directive of the President issued through the National Security Council. Where a violation of criminal statutes may be involved, Departments will refer any such case promptly to the Department of Justice.

---

[4] NSC Directive I (E).

[5] E.O. 11652, sec. 4. [6] Ibid., sec. 13 (A).

Any system of classification would have difficulty achieving its legitimate goals without effective sanctions to deter unauthorized disclosures. The tension between the people's right to know and the government's need for secrecy is highlighted by attempts to define criminal offenses involving unauthorized dissemination of national security information.

Elliot Richardson, attorney general, testified in 1973 before Congress about the three general objectives of a system of criminal sanctions.[7] The system must "deter and, where necessary, punish unauthorized disclosure of highly sensitive information." Secondly, it should focus on disclosure of secret government information by persons "who breech the trust the public reposes in them." Yet, the sanctions should not be so great they inhibit free press and free expression. Thirdly, the system should minimize the risk of prosecutions for disclosure of information that "either should never have been classified in the first place or was no longer properly classified at the time of disclosure."

---

[7] U.S., Congress, Senate, Committee on Government Operations et al., Executive Privilege, Secrecy in Government, Freedom of Information, Hearings, Vol. 2, 93rd Cong., 1st Sess., 1973, p. 234.

The complexity of the classification system has engendered some widely held misconceptions about its workings.[8] The system can only "deter and, where necessary, punish" executive branch and contracted employees through administrative procedures.[9] No law bars a member of the public, or a reporter, from possessing, reading, disclosing or publishing a classified document, unless it involves codes or communications intelligence.[10] There is no other connection between the administrative security classification system and criminal espionage laws.[11] The Internal Security Act of 1950 barred government officials from giving classified information to foreign agents or members of communist organizations.[12] The Act says:

> It shall be unlawful for any officer or employee of the United States or of any department or agency thereof ... to communicate in any manner

---

[8] U.S., Congress, Senate, Executive Privilege, Vol. 1, op. cit., pp. 441-3, p. 286.

[9] U.S., Congress, House, Security Classification Reform, op. cit., pp. 132, 409.

[10] 18 USC 798 bars disclosure of classified information relating to cryptography or communications intelligence.

[11] Harvard Law Review 85:1205, 1233.

[12] Internal Security Act of 1950. Statutes at Large, vol. 64 (1950).

> or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization ... any information of a kind which shall have been classified by the President ... as affecting the security of the United States ....

In 1973 Conservative Senator Strom Thurmond closely questioned Daniel Ellsberg concerning this mythical law proscribing unauthorized disclosure of classified information.[13]

> Senator Thurmond. ...Dr. Ellsberg, do you feel that anyone in the Government has authority to release classified information in direct violation of the law, and if so, why?
>
> Mr. Ellsberg. Senator Thurmond, with all respect, I must correct you.
>
> We cannot speak of the law here. There is no law governing it and that is something we must discuss if you think that is a central point.
>
> There is no question of discussing the law.
>
> Senator Thurmond. Are you taking the position that the Government doesn't have the authority to classify information?
>
> Mr. Ellsberg. I am taking the position that the executive branch is not the Government but only one branch of it and it cannot make laws for Congress.

Administrative sanctions under the order are not to be taken lightly, however. Anyone violating the

---

[13] U.S., Congress, Senate, Executive Privilege, Vol. 1, op. cit., p. 441.

classification directives could lose his job. To date, though, an administrative written reprimand is the most common penalty.[14] Daniel Ellsberg lost his Rand Corporation position after releasing the Pentagon Papers.[15] The CIA reported in 1973 the sanction it usually imposed for overclassification was an oral reprimand.[16]

Reprimands are given for a wide range of classification abuses, including overclassification. The executive order prohibits classification to conceal inefficiency or administrative error, to prevent embarrassment, to restrain competition or to prevent the release of information which does not require protection.[17] The Interagency Classification Review Committee revised its definition of classification abuse at the beginning of 1977 to exclude administrative errors.[18] Now, an abuse is a

---

[14] ICRC, 1976 Progress Report, pp. 9, 12.

[15] U.S., Congress, Senate, Executive Privilege, Vol. 1, op. cit., p. 442.

[16] U.S., Congress, House, Security Classification Reform, op. cit., p. 70.

[17] E.O. 11652, sec. 4.

[18] ICRC, 1976 Progress Report, p. 12.

> violation of the terms of Executive Order 11652.... The effect of which would be to preclude or delay the release of official information to include overclassification, unnecessary classification, classification without authority, unnecessary exemption and exemption without authority.[19]

Abuses resulted in seven administrative reprimands during the period July 1, 1976 to July 1, 1977.[20]

If administrative sanctions fail the government may turn to the Espionage Act of 1917, still the basic national security law, which forbids disclosure of "information relating to the national defense."[21] When using this law in prosecutions, the government must prove that a document correctly fits that statutory definition, not merely that it is classified.[22]

Sections 793-798 of Title 18 of the United States Code govern criminal penalties for mishandling national defense information.[23] Section 793 defines six offenses,

---

[19] Ibid.

[20] Letter from ICRC Executive Director Robert Wells, 1 September 1977.

[21] Crimes and Criminal Procedure, U.S. Code vol. 18, secs. 793-8 (1970).

[22] See: Harvard Law Review 85:1233-41.

[23] "The Espionage Statutes and Publication of Defense Information," Columbia Law Review 73 (May 1973):931-1087.

each involving conduct which could be preliminary to the acquisition of information by foreign agents. Parts (a) and (b) prohibit entering a national defense installation or obtaining or copying a document

> 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....

Part (c) makes it unlawful to knowingly receive or obtain national defense information. Part (d) forbids a person with lawful possession of or access to national defense information to willfully disclose such material to anyone not entitled to receive it. Part (e) speaks to any unauthorized person possessing "information relating to the national defense" who delivers it to "any person not entitled to receive it." Both (d) and (e) make it a crime to retain possession of such material. Section (f) makes criminal failure to guard against loss of such information or, if lost, failure to report it. The final section (g) makes it a crime to conspire to violate any of the sections. Violations are punishable by a $10,000 fine or 10 years imprisonment, or both.

Sections (d) and (e) raise most questions.

According to Professor Benno Schmidt:[24]

> These two provisions are undoubtedly the most confusing and complex of all the federal Espionage Statutes. They are also the statutes posing the greatest potential threat to newspapers' and reporters' obtaining and printing national defense information. The legislative drafting is at its shotgun worst precisely where greatest caution should be exercised. Moreover, legislative history suggests a basic and continuing Congressional misunderstanding of the effects achieved.

Section 794 of the Act makes criminal the communication of defense-related information to a foreign agent if the communication is "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation."

Sections 795-797 forbid photographic or graphical representation of any military installation or equipment to be disseminated publicly.

Section 798, added in 1950 by the Internal Security Act, makes criminal to "knowingly and willfully communicate" information concerning cryptographic matters.

## Judicial Background

The original purpose and whole thrust of the

---

[24]Franck and Weisband, p. 196.

Espionage Act is to catch spies, not reporters and editors. Professor Schmidt questioned certain sections of the Act, asking, for example, what is "information relating to the national defense."[25]

Senator Ablert B. Cummins expressed reservations regarding the breadth of the phrase while provisions of the act were originally being debated.

> Now I do not know, as I have said a great many times, what does relate to the public defense, and no human being can define it ... it embraces everything which goes to make up a successful national life in the Republic. It begins with the farm and the forest, and it ends with the Army and Navy.[26]

*The Supreme* Court did not come to grips with the definition until January 1941.[27] Mikhail Gorin paid a civilian investigator for the Navy to turn over to him the contents of reports on Japanese espionage activities in the United States. Gorin was not a particularly careful spy. He sent a suit to the cleaners with some of the papers in the pocket. He was arrested, convicted and sentenced to six years.

---

[25] Columbia Law Review 73:931-1087.

[26] Wise, p. 142.

[27] Gorin v. U.S., 312 US 19 (1941).

The Supreme Court reached three important conclusions. First, it ruled the espionage statute was not unconstitutionally vague.[28] Prohibitions against obtaining or delivering to foreign powers national defense information required proof of intent or reason to believe disclosure would injure the nation or aid a foreign country. The decision was not based on a strict reading of the act and the decision hung upon a comma, or lack of one. Sections 793 (d) and (e) list prohibited items plus "information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation." Failure to insert a comma after "national defense" causes the subsequent "intent" wording to modify only "information." When Congress added this wording in 1950, they intended the "reason to believe" phrase to modify only "information relating to national defense," meaning to expand coverage to oral communication.[29]

Secondly, the Court defined national defense as "a

---

[28] 312 US 19 at 27.

[29] U.S., Congress, Senate, S. Rept. 2369, 81st Cong., 2d Sess., 1950, p. 8.

generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[30] Finally, it said the jury had to decide whether the information is of the defined kind.[31] In other words, just because the information was classified didn't mean it related to the national defense. However, the fact information was not classified may be grounds for holding information doesn't relate to the national defense.[32]

Gorin did not involve any question as to where the press stood in relation to the statute. That decision burst upon the world thirty years later in the Pentagon Papers case (New York Times Co. v. U.S.).[33] However, the case turned on the question of prior restraint and the government did not even cite the espionage statutes.[34] Instead, Solicitor General Erwin Griswold argued the courts were no more equipped than the press to decide what would

---

[30] 312 US 19 at 28.

[31] Ibid., at 32.

[32] U.S. v. Drummond, 354 F2d 132 (2d Cir. 1965) at 151, cert. den., 384 US 1013 (1966).

[33] 403 US 713 (1971). [34] Cox, p. 132.

or would not damage national security.[35] The Times/Post lawyers countered they had heard statements of feared events if the Papers were published but no calamity had befallen the country.[36] In June 1971, the Court voted 6-3 in favor of the newspapers. But the decision contained ominous warnings for the press.

Justices Stewart and White, voting with the majority, cited sections of the espionage laws they felt could be applied to the press in criminal prosecution.[37] Justice White said, in part, concurring:[38]

> I do not say that in no circumstances would the First Amendment permit an injunction against publishing information about government plans or operations. Nor, after examining the materials the government characterizes as the most sensitive and destructive, can I deny that revelation of these documents will do substantial damage to public interests. Indeed, I am confident that their disclosure will have that result. But I nevertheless agree that the United States has not satisfied the very heavy burden which it must meet to warrant an injunction against publication in these cases....

Then Justice White almost invited further government prosecution:[39]

---

[35] Ibid. [36] Ibid., pp. 132-3.

[37] 403 US 713 at 735-8. [38] Ibid. at 731.

[39] Ibid. at 733.

> But failure by the government to justify prior restraints does not measure its constitutional entitlement to a conviction for criminal publication. That the government mistakenly chose to proceed by injunction does not mean that it would not successfully proceed in another way.... If any of the material here at issue is [covered by espionage laws] the newspapers are presumably now on full notice of the position of the United States and must face the consequences if they publish.

There is the question of whether Congress intended Section 793 to apply to newspapers at all.[40] The statute contains no express exemption from the Act for the press but speaks only of "communicating, delivering or transmitting" information.[41] Subsequent sections specify "publish."[42] Justice White in New York Times said "communicates" is not broad enough to encompass publication. Legislative history shows Congress was sensitive to the importance of not restricting freedom of the press. Both Houses deleted portions of the Espionage Act which would punish the act of publishing defense information without intent.[43]

Five days after the decision, Daniel Ellsberg and

---

[40] Harvard Law Review 85:1237; Cox p. 140.

[41] 18 USC 793 (e). [42] 18 USC 794 (b).

[43] Congressional Record 55:3131-44 (1917).

Anthony Russo were indicted for stealing government property, failing to return it and conspiracy. This was the first time information was claimed as government property.[44] Ellsberg had made copies and returned the original documents. All the questions about classified national security information withered on the vine when the case was dismissed because of governmental improprieties.[45]

The Ellsberg and Russo case brought renewed calls for Congressional action to rewrite the espionage laws. Assistant Attorney General Antonin Scalia, testifying before a Senate Judiciary subcommittee on Congressional access to information in 1976, said:[46]

> The current laws prohibiting and punishing the disclosure of national security information are patently inadequate. Most of them require the demonstration of a positive intent to harm the United States, which is always difficult to establish factually and which may not technically exist in the case of disclosures by individuals

---

[44] Cox, p. 138.

[45] The White House "plumbers" burglarized the office of Daniel Ellsberg's psychiatrist in an attempt to damage Ellsberg's reputation. See: Cox, p. 135; "Text of Judge Gesell's Decision in the Ellsberg Case," New York Times, 25 May 1974.

[46] U.S., Congress, Senate, Congressional Access, op. cit., p. 108.

> who are merely following their own conception of what is good for the country, however much that may differ from what their fellow citizens, through their elected representatives, may have established.

The government has shown concern about the failure of Congress to provide adequate sanctions against persons who make unauthorized disclosures,[47] but when given the chance to suggest wording for a law, security expert William Florence said that a DOD spokesman came up blank. The spokesman admitted a classification mark is only part of the evidence tending to show information would endanger national security if disclosed in an unauthorized manner. The spokesman said, "... There is no way a departmental directive could predetermine that the unauthorized disclosure should subject an individual to criminal prosecution."[48]

## Secrecy Agreements

The battle between government and press concerning publication of classified information remains unresolved.

---

[47] U.S., Congress, House, Security Classification Reform, op. cit., pp. 223-29.

[48] "Recommendation on Handling Classified Materials," Congressional Record 120:41699 (1974).

Most government employees are effectively deterred by administrative sanctions from releasing such information.[49] Nonetheless, it seems the government is free to guard its secrets as best it can, and the press is free to ferret out and publish what it can.[50]

President Carter apparently feels too many secrets are being exposed and has referred several times to the need to stop leaks. He suggests reducing the number of individuals in the executive branch and Congress with access to classified information. Rather than imposing criminal penalties for unauthorized disclosure, President Carter wants to control more tightly the secret data.[51] CIA Director Admiral Stansfield Turner would clamp down on both those who disclose and those who receive.

> What I'm concerned with is that if a member of the Department of Agriculture today releases information on crop futures that will help somebody make some money, he can go to jail. If a member of the intelligence community releases information vital to the security of this country,

---

[49] Dorsen and Gillers, pp. 95, 224-30.

[50] See: Henkin, p. 277.

[51] St. Louis Post-Dispatch, 15 March 1977, editorial.

it's very difficult for us to find any way to discipline him.[52]

Indeed, in at least 41 statutes Congress has restricted the release of information by executive agencies, their employees, or officials.[53] These statutes protect information in four general categories: (1) industrial property rights (trade secrets, patentable inventions); (2) information which could be improperly used by speculators; (3) individual's personal information; (4) national defense.

Having found it difficult to use the espionage statutes to protect the unauthorized disclosure of classified national security information, the executive has discovered a new way to guard against release of such information--secrecy agreements.

Congressional examination of U.S. foreign intelligence activities prompted President Gerald Ford to issue in 1976 Executive Order 11905, outlining boundaries for

---

[52]"Turner: Law May Be Needed To Impede Security Leaks," Congressional Quarterly Weekly Report 35 (26 March 1977):585.

[53]U.S., Congress, House, Availability of Information to Congress, op. cit., pp. 99-101; FoI Act Exemptions, 5 USC 552.

intelligence agencies.[54] Section 7 states guidelines for secrecy protection.

> (a) In order to improve the protection of sources and methods of intelligence, 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 [read employment], sign an agreement that they will not disclose that information to persons not authorized to receive it.

The name of any person who violates the agreement is sent to the agency head for disciplinary action and to the attorney general for legal action.

The use of a secrecy agreement, a legal contract, to protect secret data *and* impose sanctions probably results from the outcome of the Victor Marchetti case.[55] Former CIA agent Marchetti wrote a book, The CIA and the Cult of Intelligence, which the agency attempted to partially suppress. Upon joining the CIA, Marchetti promised

> not to divulge in any way any classified information, intelligence or knowledge, except in the performance of his official duties, unless

---

[54] U.S., President, Executive Order 11905, "United States Foreign Intelligence Activity," Federal Register 41:7701.

[55] U.S. v. Marchetti, 466 F2d 1309 (4th Cir., 1972).

> specifically authorized in writing by the Director or his authorized representative.[56]

A similar oath was required when Marchetti resigned.

In September 1972, Fourth Circuit Judge Clement Haynsworth held classification was an appropriate tool in providing protection of intelligence sources and methods, and the secrecy agreement was a binding, legal contract. He said, "The government's need for secrecy in this area lends justification to a system of prior restraints against disclosure by employees of classified information obtained during the course of employment."[57]

A sequel to this case, Knopf v. Colby, was settled in February 1975.[58] Despite passage of a Freedom of Information Act amendment during the intervening years which allows judicial review of classified documents, the outcome of the case remained the same. Judge Haynsworth wrote:[59]

> ... The First Amendment is no bar against an injunction forbidding the disclosure of classified information within the guidelines of Executive

---

[56] Ibid., see p. 1312 for a copy of the secrecy agreement and oath.

[57] Ibid., at 1316-7.

[58] Alfred A. Knopf, Inc. v. Colby, 509 F 2d 1362 (4th Cir. 1975).

[59] Ibid., at 1370.

> Orders when (1) the classified information was acquired, during the course of his employment, by an employee of a U.S. agency or department in which such information is handled and (2) such 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.

The executive branch continues its efforts to find some means of imposing criminal sanctions. Supreme Court dicta in Times v. U.S. points the way for the executive to try to use the Espionage Act, but the executive, perhaps wisely considering the Act's confused wording, has thus far not done so. For the present, it appears the executive is without criminal sanctions to impose against those who disclose national security information unofficially. The Marchetti case led the search for sanctions into the realm of contracts and the executive successfully prevented the disclosure of some classified information.

The classification system is about to be revised by President Carter. The next chapter describes the new plan and its method of providing protection for classified national security information.

## CHAPTER VII

## THE CARTER PLAN

President Jimmy Carter has surprised the press and intelligence organizations with a national security first--publicly circulating a draft executive order revising the classification system.[1] Comments on the order were due October 14, 1977, with the order to become effective March 1, 1978.[2]

Entitled "National Security Information and Material," the order's purpose is "to mold a manageable classification system that will provide greater openness in government while at the same time effectively protecting sensitive national security information."[3] This will be

---

[1] "Draft Executive Order Being Circulated Would Revise Classification Procedures," Access Reports 3 (20 September 1977):1.

[2] Ibid., This article contains the text of the Carter draft order.

[3] William M. Nichols, cover letter to the Carter draft order, September 13, 1977.

accomplished, according to the order's cover letter, "by establishing stricter and more definitive standards than presently exist for the classification of national security information."

The move to rewrite E.O. 11652 was begun under President Ford but the study was dropped after the November 1976 elections.[4] President Carter formed his own task force to review the classification system and bring it in line with experience gained under the Freedom of Information Act.[5] In announcing the review, Presidential Counsel Robert J. Lipshutz suggested the government had "gone far beyond the bare minimum" of classification needed to protect the nation's security.[6]

Mark Lynch of the American Civil Liberties Union (ACLU) initially reacted cautiously to the new order. He praised the administration for making the order public but said it is "not readily comprehensible, nor readily

---

[4] "Task Force To Be Formed To Study Classification System," Access Reports 3 (4 May 1977):5.

[5] Ibid.

[6] "Washington Focus," Access Reports 3 (1 June 1977):1.

readable."[7] After studying the draft order, however, the ACLU found it "not appreciably different from its seriously flawed predecessor" and "even worse ... in several respects."[8]

The new order melds portions of Executive Order 11652 and the National Security Council implementing directive into a revised system with two crucial changes. First, four years are cut from the time government can keep most top secrets.[9] Instead of a graduated declassification system, all classifications are good for six years, then the information is declassified, except when there is "a need, directly related to the national security, to continue classification ...."[10]

Secondly, employees who require access to classified information must sign a secrecy agreement "as a precondition of access to classified information."[11] Gary

---

[7] "Draft Order Being Circulated Would Revise Classification Procedures," Access Reports 3 (20 September 1977): 1.

[8] "Carter Secrecy Plan Called Worse Than Nixon's," Columbia Daily Tribune, 15 October 1977.

[9] U.S., President, "National Security Information and Material," (Draft), 13 September 1977, sec. 2 (f) (1). (Hereinafter: Draft order).

[10] Draft order, sec. 2 (f) (2). [11] Ibid., sec. 6 (b).

Barron, a National Security staff member who helped write the draft order, said the secrecy agreements were "a thing the lawyers did. The whole idea was to have something uniform. This was not put in there to enjoin any publications. That was not the intent."[12]

The remainder of this chapter considers what the Carter order says, section by section, where it differs from E.O. 11652, and some of the implications of the changes.

## Definitions

The preamble to the draft order states simply the legal basis for establishing the classification system: "By virtue of the authority vested in me by the Constitution and statutes of the United States of America ...." The Freedom of Information Act exemption (b) (1) is not specified as it was in the preamble to the Nixon order.

Section 1 of the draft order lists definitions. The Carter order continues to use the term "national security" but changes one word in the definition. National security is "the foreign policy or national

---

[12] "Carter Aides Draft Secrecy Rules Shift," New York Times, 15 September 1977, p. A18.

defense interests of the United States." (Emphasis added.) Congress was greatly concerned that the Nixon order uses "foreign relations", a term Rep. Moss thought broader than "policy."[13]

The order defines classified information as "official information which has been determined by proper authority to require a degree of protection in the interest of national security ...."[14]

## Classification

The draft order retains three categories of classification---Top Secret, Secret and Confidential. The first two classifications carry definitions similar to those in E.O. 11652. Unauthorized disclosure of Top Secret information "could reasonably be expected to cause exceptionally grave damage to the national security."[15] Secret applies to information the unauthorized disclosure of which "could reasonably be expected to cause serious damage to the national security."[16] The definition for Confidential would be tightened. Instead of information that could

---

[13] H. Rept. 93-221, pp. 62-4.

[14] Draft order, sec. 1 (f). [15] Ibid., sec. 1 (f)(1).

[16] Ibid., sec. 1 (f)(2).

"cause damage," information so classified would be expected to "cause significant damage."[17]

Unlike the Nixon order, the Carter draft order lists 13 criteria a classifier must consider before affixing a classification.[18] The order says that if information is classifiable, its unauthorized disclosure could reasonable be expected to:[19]

> (1) Make the United States or its allies vulnerable to attack by a foreign power, or weaken the ability of the United States or its allies to conduct armed operations or defend themselves, or diminish the effectiveness of the United States' armed forces; or
>
> (2) Lead to hostile political, economic, or military action against the United States or its allies by a foreign power; or
>
> (3) Disclose, or provide a foreign nation with an insight into, the defense plans or posture of the United States or its allies; provide a foreign nation with information upon which to develop effective countermeasures to such plans or posture; weaken or nullify the effectiveness of a United States military, foreign intelligence, or foreign counterintelligence, plan, operation, project, or activity; or
>
> (4) Aid a foreign nation to develop, improve, or refine its military potential; or
>
> (5) Reveal, jeopardize, or compromise an intelligence source or method, an analytical

---

[17] Ibid., sec. 1 (f)(3).

[18] Ibid., sec. 2 (1).

[19] Ibid., sec. 2 (b)(1-13).

technique for the interpretation of intelligence data, or a cryptographic device or system; or

(6) Disclose to other nations or foreign groups that the United States has, or is capable of obtaining, certain information or material concerning those nations or groups without their knowledge or consent; or

(7) Deprive the United States of a scientific, engineering, technical, economic, or intelligence advantage directly related to national security; or

(8) Create or increase international tensions; or otherwise significantly impair our foreign relations; or

(9) Disclose or weaken the position of the United States or its allies in the discussion, avoidance, or peaceful resolution or existing or potential international differences; or

(10) Disclose plans prepared by, or under discussion by, officials of the United States to meet contingencies or situations arising in the course of our foreign relations or national defense; or

(11) Cause political or economic instability or civil disorder in a foreign country; or

(12) Disclose the identity of a confidential source of a United States diplomatic or consular post; or

(13) Disclose information or material provided to the United States in confidence by a foreign government or international organization.

Though the Carter draft order specifies these categories of classifiable information, it offers no real change from E.O. 11652. The listing covers the spectrum of currently classifiable information. And many of the categories are phrased broadly, such as information which could "create or increase international tensions" (no. 8). An American Civil Liberties Union spokesman said the

AD-A051 506 AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OHIO F/G 5/4
THE NATIONAL SECURITY CLASSIFICATION SYSTEM.(U)
DEC 77 R L OBORN
UNCLASSIFIED AFIT-CI-78-22 NL

3 OF 3
AD
A051 506

END
DATE
FILMED
4-78
DDC

phrasing of the categories is so inclusive "that it is hard to imagine any government information pertaining to national defense and foreign relations that could not fit within one."[20]

In section 2 (c), the draft order lists types of information which are not to be classified. Of the seven prohibitions, two urge officials to opt for the less restrictive treatment if there is some question as to what classification should be applied. The order requires the classifying official "strike the balance in favor of public access to official information ...."[21]

Other prohibitions to be considered by the classifier include not classifying information "in order to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency ...;"[22] not classifying information resulting from "independent or nongovernmental research and development ...;"[23] not classifying documents solely on the basis

---

[20] Columbia Daily Tribune, 15 October 1977.

[21] Draft order, sec. 2 (c)(1).

[22] Ibid., sec. 2 (c)(2).

[23] Ibid., sec. 2 (c)(4).

of reference to a previously classified document;[24] classification shouldn't be used only for "the purpose of limiting dissemination of information which is not classifiable under the provisions of this Order;"[25] and not classifying "basic scientific research information ... except for such information that is directly related to the national security."[26]

The latter prohibition would seem to please the scientists until they realize the exception clause encompasses probably everything that is currently classified.

Section d, Classification Authority, like the Nixon order, requires original classification authorities to be designated by the president in writing. Both the Carter and Nixon orders list 12 departments and agencies whose heads receive Top Secret classification power.[27] However, the Nixon order specifically gives the president the option

---

[24] Ibid., sec. 2 (c)(5).

[25] Ibid., sec. 2 (c)(6).

[26] Ibid., sec. 2 (c)(3).

[27] See: Carter draft order, sec. 2 (d)(1); E.O. 11652, sec. 2 (A)(3).

to designate individuals within the Executive Office of the President as Top Secret classifiers. The Carter draft order does not.

The Carter draft order lists six agencies whose heads receive original Secret classifying authority[28] and three agencies whose heads receive Confidential classifying authority.[29] An individual empowered to classify at a particular level also has the right to assign original classifications at lower levels. The Nixon order specified 25 classifying organizations; the Carter draft names 21.

The Carter order allows delegation and redelegation of classification authority if it is in writing and granted to officials by name or title of position held.[30] Therefore, the redelegation power seems unlimited, though the order does request delegation be "restricted to those officials whose duties and responsibilities necessitate the origination of classified information on a regular and recurring basis."[31]

---

[28] Draft order, sec. 2 (d)(2).

[29] Ibid., sec. 2 (d)(3).

[30] Ibid., sec. 2 (d)(4).

[31] Ibid.

## Exceptions

All classifications are given a six-year life under the Carter draft order.[32] However, each original classification authority is asked at the time of classification to set a "specific date or event for automatic declassification of the information ... as early as the national security interest will permit."[33] The date or event cannot exceed six years.

The order does recognize the need to protect some information past the six year mark.[34] Only Top Secret classification authorities may set a later date or event for automatic declassification. The date or event cannot exceed 20 years from the date of original classification; the information must then be reviewed for possible declassification.[35] The classification can be extended subsequently for 10 year intervals.[36] Extending a classification past six years requires lower-authorized classifiers to seek out Top Secret classifiers.

---

[32] Ibid., sec. 2 (f)(1).

[33] Ibid.

[34] Ibid., sec. 2 (f)(2).

[35] Ibid.

[36] Ibid., sec. 4 (d).

Gary Barron, National Security Council staff member, said, "hopefully someone with Top Secret authority would be more responsible and say no."[37]

The Nixon order contains the same requirement to seek out a Top Secret classifier in order to exempt classified information from the automatic declassification schedule.[38] However, the Nixon order lists four general exemption categories while the Carter draft order requires the reasons for extended classification "be specific and must explain why the classification will continue to meet the requirements set forth in subsection 2(a) above."[39]

Top managers, familiar with the Nixon exemption categories, are likely to formulate several variations of the reasons used to exempt classified information under the current order and apply those reasons via a myriad of rubber stamps in place of the Carter order call for individualized explanations for each extension. Some such circumvention of the required Carter order explanations will probably be necessary or a whole new strata of classification administrators will arise---those tasked

---

[37] New York Times, 15 September 1977, op. cit.

[38] Draft order, sec. 5 (b). [39] Ibid., 2 (f)(2).

with originating specific reasons and writing explanations for continuing the classification of certain types of information.

Classification extensions will probably be needed for a large volume of "sources and methods" information, that gleaned by cryptography, communication intercepts and satellite photography, most currently, routinely exempted from the declassification schedule. Such a large percentage of classifications made by the Department of Defense, the Central Intelligence Agency and the Energy Research and Development Administration are currently exempted from automatic declassification that the Interagency Classification Review Committee doesn't receive declassification/exemption data from those organizations.[40]

The Carter draft order requires each classified document show on its face: "(i) the identification of the original classification authority; (ii) the office of origination; (iii) the date of origination; (iv) the date or event for declassification or review; and (v) one of the three classification designations defined herein."[41]

---

[40] ICRC, 1976 Progress Report, p. 21.

[41] Draft order, sec. 2 (g)(1).

Continuing, the order states, "No other designations, e.g., 'For Official Use Only,' "Limited Official Use,' shall be used to identify information requiring protection in the interest of national security ...."[42] Such prohibitions would seem to halt the use of all the extra markings that so confused certain congressmen during the House subcommittee's hearings in 1971 and 1972.[43] (See Chapter V, subhead: Access and Distribution Markings.) But the Carter order does not forbid additional markings to be used as access and dissemination markings.[44] The important phrase is "to identify information requiring protection in the interest of national security ...." Once one of the three classifications does that, any additional marking may be applied to limit access and dissemination.

Also, the Carter draft order requires each classified document to indicate which portions are classified and at what level in order to facilitate exerpting.[45] Classified information received from a foreign government or international organization retains its own classification

---

[42]Ibid. [43]H. Rept. 93-221, pp. 75-8.

[44]Draft order, sec. 2 (g)(4).

[45]Ibid., sec. 2 (g)(2).

or is protected at an equivalent level.[46]

Any information needing special dissemination and reproduction limitations "shall be clearly annotated to place the recipient on notice to restrict dissemination and reproduction," and the following notice is to be included on the document:[47]

> Reproduction of this document or portions thereof is prohibited without authorization of the originating office. Its further dissemination shall be restricted to those authorized by the addressee.

## Derivative Classification

The Carter draft order explicitly recognizes derivative classifications and gives a warning regarding their use.[48] Persons who "reproduce, extract, summarize or otherwise use classified information" are not given original classification authority. Anyone who applies a classification derived from another source is directed to "verify the current need for and level of classification of the information or material prior to applying such markings." Also, the newly created document is to carry

---

[46] Ibid., sec. 2 (g)(3).

[47] Ibid., sec. 2 (g)(4). [48] Ibid., sec. 3.

the dates or events assigned by the originator, thus precluding continued classification of information in the new document when it is declassified in the original.

This section on derivative markings presents two major problems. First, from the practical standpoint, it is almost impossible to "verify the current need" for every piece of information extracted from the original document for use in another document. Information may originally come from several sources, should each be contacted to verify the classification? What of documents produced on a daily basis for internal use of some particular military command but which receive no distribution outside that command?

## Declassification

Section 4 of the Carter draft order is entitled Declassification. The first sentence reads: "Declassification of classified information shall be given emphasis comparable to that accorded to classification." Without a truly automatic declassification system, only time, money and manpower can produce results in accord with that statement. The Carter order provides automatic declassification but allows exemptions, as did earlier orders. In

an attempt to prompt declassification, the Carter order adds several new practices.

The draft order emphasizes the decision to declassify will not be made on the basis of the level of classification assigned a particular document, but will be made on the "expected perishability and loss of the sensitivity of the information with the passage of time, and with due regard for the public interest in access to official information."[49] The Nixon order bases downgrading and classification upon the original classification. Under the Carter draft order, a decision not to declassify material should be made only if release of the information would be "demonstrably harmful to the national security."

The Carter draft order lowers the time period when all classified information must be reviewed for continued classification from 30 to 20 years. Using declassification guidelines from various agencies, the Archivist of the United States has the responsibility for overseeing declassification of this older information. It will take a few years before the Archives can reach the 20-year mark, it is just now catching up to the 30-year limit

---

[49] Ibid., sec. 4.

established by the Nixon order.[50] Only the head of an agency can authorize extension of classification past 20 years. Extended classification must be reviewed each succeeding 10 years.[51]

The Carter draft order recognizes that review of classified information more than 20-years old could be a prodigious task, and authorizes review of "only that information constituting the permanently valuable records of the Government ...."[52]

Mandatory review will be available for all classified information, not just material more than 10-years old as prescribed by the Nixon order.[53] Only material originated by a President or White House Staff will be protected for 10 years.[54] The manner in which a review is started remains similar to the current order. A review request may come from the public or an agency, but the request must "describe the material sufficiently to enable the agency having custody to locate it with a reasonable

---

[50] U.S., Congress, House, Hearings, Appropriations for Fiscal Year 1977, op. cit., p. 191.

[51] Draft order, sec. 4 (d). [52] Ibid.

[53] Ibid., sec. 4 (e). [54] Ibid., sec. 4 (e)(4).

amount of effort."[55]

Information originated by a foreign government or an international organization will be allowed to rest 30 years before being reviewed.[56]

Authority to downgrade and declassify will reside with the official who authorized the original classification. The authority is also to be granted to "additional officials at the lowest practical echelons of command and supervision ... particularly with respect to information within their areas of responsibility."[57] This attempt to extend declassifying authority to lower echelons represents a commitment to ensure timely downgrading and declassification. The outcome could result in the appointment of more declassifiers than classifiers.

While the Carter draft order protects a president's papers while he remains in office, once the presidential term expires the Archivist of the United States

> shall have the authority to review, downgrade and declassify information which was classified by the President, his White House staff, special committees or commissions appointed by him or

---

[55]Ibid. [56]Ibid., sec. 4 (f).

[57]Ibid., sec. 4 (g)(2).

> others acting in his behalf when this information is not part of the records of an agency subject to Federal record statutes.[58]

Section 5, Downgrading, of the Carter draft order provides for changing a classification to a lower level. Under the current order, downgrading occurs as a part of the automatic process. Little downgrading will probably occur under the Carter order because (1) none is required and (2) since all classifications are good for only six years, unless exempted, there will be little need to review information for downgrading in any wholesale fashion.

## Secrecy Agreements

Section 6, Safeguarding, of the Carter draft order shifts responsibility for issuing implementing directives from the National Security Council to the newly created Security Information Oversight Office. One policy the directives must conform to involves granting access to classified information.[59] The order states:

> No person shall be given access to classified information unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of official duties.

---

[58] Ibid., sec. 4 (g)(7). [59] Ibid., sec. 6 (a)(1).

This statement opens the door to the need for security clearances as a prerequisite for obtaining a job.

Perhaps the premier innovation of the Carter draft order is the requirement for the "signing of a secrecy agreement as a precondition of access to classified information."[60] It appears if a person is unwilling to sign such an agreement, that person will not get the job. The use of a secrecy agreement probably results from the outcome of the Marchetti and Knopf cases. (See Chapter VI.) Employees who disclose information without authorization could be prosecuted for breach of the secrecy contract and the government would not have to attempt to use the ambiguous Espionage Act. The secrecy agreement will in effect close the loophole through which Daniel Ellsberg and Anthony Russo were able to escape with the Pentagon Papers.

Chairman of the House Government Information subcommittee, Rep. Richard Preyer, called the secrecy agreement provision "singularly objectionable."[61] Preyer protested the use of the procedure government-wide would

---

[60] Ibid., sec. 6 (b).

[61] Columbia Daily Tribune, 15 October 1977, op. cit.

have a chilling effect on potential "whistle blowers."

## Special Access

The Carter draft order allows the head of an agency to impose "special requirements with respect to access, distribution, and protection of classified information."[62] Such special access programs deal with communications and satellite intelligence. Thus, the Carter order does not differ from the Nixon order in allowing the use of access, distribution and control markings.

However, there is a difference in the handling of the special programs. Under the Carter draft order, only the head of an agency may create a special access program; and he must do so in writing. For such a program to be created, three criteria must be met:[63]

> (i) Normal safeguarding procedures are not sufficient to limit need-to-know or access;
> (ii) the number of persons who will need access will be reasonably small and commensurate with the objective or providing extra protection for the information involved;
> (iii) the special access controls balance the need to protect the information against the full spectrum of needs to use the information.

Once the Carter order takes effect, agency heads

---

[62] Draft order, sec. 6 (c)(1). [63] Ibid.

must review existing special access programs and maintain a central list of all such programs they create or continue.[64] Further, special access programs will automatically end every three years unless specifically renewed.[65]

Historical researchers and former officials may be granted access to classified information if that access is "consistent with the interests of national security;" if reasonable action is taken to ensure "that properly classified information is not subject to unauthorized disclosure;" and for a former official, if that person is given access only to those "papers which the former official originated, reviewed, signed or received while in public office."[66]

## Administration

The draft order establishes a new set of administrators for the classification system.[67] Overall policy direction will rest, as it does now, with the National Security Council. However, the Administrator of General Services will be responsible for implementing and monitoring

---

[64] Ibid., sec. 6 (c)(3). [65] Ibid., sec. 6 (c)(2).

[66] Ibid., sec. 6 (d)(1-3). [67] Ibid., sec. 7.

the program.[68] The order will establish a Security Information Oversight Office, headed by a full-time director with a permanent staff, which will oversee agency actions, hear complaints, develop implementing directives and report annually to the president.[69] The Oversight Office supercedes the Interagency Classification Review Committee (ICRC), and in so doing, places oversight in the hands of bureaucrats where it was formerly in the hands of individuals from the very agencies that produced most classified material.

An Interagency Security Information Advisory Committee will be created and composed of the current ICRC membership. The Committee will be chaired by the Director of the Oversight Office.[70] The Committee will advise the Director of the Oversight Office in matters related to the Carter order's implementation.

Section 8 of the Carter draft order is entitled Administrative Sanctions. The first paragraph reads:

---

[68] Ibid., sec. 7 (a)(1).

[69] Ibid., sec. 7 (a)(1)(i-iv).

[70] Ibid., sec. 7 (b)(2).

> Any officer or employee of the United States who knowingly and willfully classifies or continues the classification of information in violation of this Order or any implementing directive; or knowingly and willfully and without authorization, discloses classified information through gross negligence; or knowingly and willfully violates any other provision of this Order or implementing directive which the head of an agency determines to be a serious violation, shall be subject to appropriate administrative sanctions. In any case in which the Oversight Office finds that unnecessary classification or overclassification has occurred it shall make a report to the head of the agency concerned so that corrective steps may be taken.

The order lists the sanctions which may be applied.[71] The sanctions may include "reprimand, suspension without pay, removal, or other sanctions in accordance with applicable law and agency regulations. This section on sanctions concludes with a reminder that the Department of Justice shall be informed of "any case in which a violation of the criminal law may be involved."[72]

Representative Preyer has already noted some of the deficiencies of the Carter draft order, and Congress is likely to find several more. Congress had no major say in the writing of the order and the order does not solve some of the problems identified in previous orders. Like the

---

[71] Ibid., sec. 8 (b). [72] Ibid., sec. 8 (c).

Nixon order, the Carter draft order forbids overclassification and unnecessary classification and establishes declassification procedures. But also like the Nixon order, the Carter draft order fails to completely define national security.

This chapter examined the major portions of the Carter draft order and differences and similarities with the current order governing classification of information. The Carter order largely resembles the current system but alters the constituency of the committee which oversees the order's implementation, shortens the length of time prior to declassification, and adds government-wide use of a secrecy agreement.

Nonetheless, the management and operation of the classification system will stay firmly within the executive branch; no Congressional oversight is called for. The next chapter briefly explores Congressional action in the classification realm.

## CHAPTER VIII

## OTHER PLAYERS

Thus far, this study has explored the secrecy or disclosure dilemma, has traced the history of the executive classification system and has considered current and impending executive orders which govern the system's operation. The executive branch has had basically a free hand in dealing with classified information. Though Congress has the power to control the system, it has not done so despite repeated recommendations by its own committees.[1] But if Congress declines to make a frontal attack on the secrecy system, it has imposed public access to official records and increased its own power to oversee those who produce secrets. An in depth discussion of congressional activities in the secrecy area is outside the scope of this study but a brief summary of actions will allow a glimpse of the current Congressional concerns.

---

[1] See: H. Rept. 93-221, pp. 23-7, 100-104.

## Freedom of Information Act (FOIA)

After more than a decade of debate, Congress produced the Freedom of Information Act of 1966.[2] The Act as a whole establishes a presumption in favor of disclosure. The Act covers access to governmental records and provides a person with the courts as an avenue to access. The burden of proof for need of secrecy lies with the government.

However, the Act listed nine exemptions to disclosure. The first applied to matters "specifically required by Executive Order to be kept secret in the interest of the national defense or foreign policy."[3] This exemption was premised upon the concept some government information must be kept secret for the security and well-being of the nation. The wording left the judiciary with a limited role in cases involving nondisclosure for

---

[2] 5 USC 552. For further discussion of the Act, the salient points of which are here paraphrased, see: Barker, pp. 16-8; Yale Law Journal 84:743; Yale Law Journal 85:401.

[3] Freedom of Information Act, 5 USC 552 (b)(1) (1966).

national defense or foreign policy reasons.[4]

Two cases in particular prompted Congress to revise that first exemption. In Epstein v. Resor a lower court said its role was limited to determining whether the material in question was covered by an appropriate executive order and if so, whether the classification was arbitrary and capricious. No inspection of documents was necessary.[5]

Secondly, the Supreme Court held in Environmental Protection Agency (EPA) v. Mink the exemption reflected congressional intent to defer to executive decisions concerning the need for withholding documents.[6] If a document was classified in a proceduraly correct manner, the substance of the classification was not subject to judicial review. A government official's affidavit attesting to proper classification was sufficient proof of procedural adequacy.[7] Justice Stewart said, concurring,

---

[4] H. Rept. 93-221, p. 28; James M. Gorski, "Access to Information? Exemptions From Disclosure Under the Freedom of Information Act and the Privacy Act of 1974," Willamette Law Journal 13 (1976):135, 142.

[5] 421 F2d 930 (9th Cir. 1970).

[6] 410 US 73 (1973).

[7] H. Rept. 93-221, p. 30.

Congress did not provide "means to question any Executive decision to stamp a document 'secret,' however cynical, myopic, or even corrupt that decision might have been."[8] Finally the Court said Congress could have legislated its own classification procedures. Congress had chosen to accept executive determination of what should be classified. It was not obligated to do so.[9]

Congress moved to correct the deficiency when it passed a series of amendments in October 1974.[10] One specifically authorized judicial review of contested materials in camera (judge's chambers). In November 1974, President Ford vetoed the amendments, saying, "the courts should not be forced to make what amounts to the initial classification decision in sensitive and complex areas where they have no particular expertise."[11] Congress overrode the veto on November 20.

Exemption (b) (1) now allows federal courts to determine whether matters are

---

[8] 410 US 73 at 95. [9] Ibid., at 83.

[10] Yale Law Journal 85:401.

[11] Kansas City Star, 21 October 1974.

> specifically authorized under criteria established by Executive order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive order.[12]

The government must be given a chance to defend its position before in camera inspection is ordered.[13] Additionally, the courts are authorized to separate "any reasonable segregated portion of a record ...."[14] The Carter order which requires marking each paragraph with appropriate classification should make the court's job easier.

The courts share some of President Ford's concern regarding original classification decisions, but congressional debate about the amendments illustrated court limits.[15] Illustrative of Congressional intent is Rep. Moorhead's comment that the classification decision must be made within the framework of the executive order's criteria:[16]

---

[12] 5 USC 552 (b)(1).

[13] U.S., Congress, House, "Freedom of Information Act Amendments," H. Rept. 93-1380, 93rd Cong., 2d Sess., 1974, p. 9.

[14] 5 USC 552 (b). [15] Yale Law Journal 85:404.

[16] U.S., Congress, House, 7 October 1974, Congressional Record 120:10007.

> Mr. Horton. This provision is not intended to permit a court free rein to classify information as it wishes, is it?
>
> Mr. Moorhead. ... A court could only determine whether the information was "properly classified pursuant to (an) Executive order." In other words, the judge would have to decide whether the document met the criteria of the President's order for classification --- not whether he himself would have classified the document in accordance with his own ideas of what should be kept secret.

Knopf v. Colby became the first case tried under the FOIA Amendments.[17] The court found it unnecessary to conduct an in camera review. The government did not have to disclose sensitive information to the court because testimony of officials and presumption officials regularly correctly apply classifications was sufficient. Judge Haynsworth said:[18]

> In our own chambers, we are ill equipped to provide the kind of security highly sensitive information should have. The national interest requires that the government withhold or delete unrelated items of sensitive information, as it did, in the absence of compelling necessity. It is enough ... that the particular item of information is classified and is shown to have been embodied in a classified document.

---

[17] 509 F2d 1362 (4th Cir. 1975).

[18] Ibid., p. 1369.

No Federal court has yet ruled on the substantive issue of whether classified material actually deserved a classification. In Halperin v. Department of State, U.S. District Judge June Green held portions of a "background" news briefing by Henry Kissinger should be released.[19] The information was classified, though originally made available at the time of the news conference. Judge Green decided the classification had not been procedurally correct.

Lower courts continue to recognize in camera inspection of documents are not required under FOIA.[20] Similarly, courts recognize "few judges have the skill or expertise to weigh the repercussions of disclosure of information."[21] And the reason:[22]

> The reluctance of Congress and the courts to require in camera inspections is well founded. In camera inspections are burdensome and are conducted without the benefit of an

---

[19] Halperin v. Department of State, 2 Media Law Reporter 2297 (1977).

[20] Weissman v. CIA, 2 Media Law Reporter 1276 (1976) and St. Louis Post-Dispatch v. FBI, (USDC-DC Civil Action 75-1025, June 1977).

[21] Weissman v. CIA, 2 Media Law Reporter 1276.

[22] Ibid., at 1279.

> adversary proceeding. A denial of confrontation creates suspicions of unfairness and is inconsistent with our traditions.

Courts are empowered under the Freedom of Information Act to review executive classification decisions but seem not anxious to become entangled as the final arbiter in the classification process.

## Congressional Alternative

All three branches of the federal government recognize the right of Congress to formulate a classification system.[23] Congress remains unable, or unwilling, to undertake so Herculean a task. Representative Moss stated the need:[24]

> There has been a marked expansion of the cult of secrecy, a feeling that you gain security through the negative policy of secrecy. I think it does require the attention of the Congress. I think we abrogate our responsibilities by leaving solely to the executive the judgment of what kinds of systems of classification we should have.

---

[23] See: H. Rept. 93-221, p. 94; EPA v. Mink, 410 US 73.

[24] U.S., Congress, Senate, Congressional Access, op. cit., p. 97.

The Congress has had success in one small area. Only one Federal agency operates under a separate statutory security classification system---the Atomic Energy Commission (now Nuclear Regulatory Commission).[25] Under the Atomic Energy Act of 1954 nuclear information is known as "restricted data."[26] The statutory system operates within the framework of E.O. 11652 and classification categories of the order are also applicable to nuclear information. Under the Atomic Energy Act, by definition, information is classified from its inception. Information is constantly being reviewed for declassification. Congress says the system is efficient.[27]

Interestingly, under the Atomic Energy Act, Congress cut itself in for a piece of the classification action.[28] Chapter 17 of the Act established a Joint Committee on

---

[25] See: H. Rept. 93-221, p. 96; "Congress Abolishes Joint Committee on Atomic Energy," Congressional Quarterly Weekly, 20 August 1977, p. 1752.

[26] 42 USC 2162. For the text of this Act, refer to the U.S. Code.

[27] H. Rept. 93-221, pp. 99, 103.

[28] Act to Amend the Atomic Energy Act of 1946, PL 83-703, 60 Stat. 755 (1954).

Atomic Energy composed of nine members from each House. Section 206 empowers the Committee to classify information originating within the Committee "in accordance with standards used generally by the executive branch ...."[29] The Committee was abolished in July 1977 and became the Office of Classified National Security Information in the Senate.[30]

Congressional failure to provide a government-wide statutory classification system does not result from lack of trying.[31] During the past couple of years, most congressional action has been aimed at providing penalties for unauthorized disclosure of national security information or establishing oversight of the agencies that produce most classified material.

---

[29] Ibid., sec. 206.

[30] U.S., Congress, Senate, 1 July 1977, Congressional Record, S. 11385.

[31] For some of the proposals during the last two years see: "Congress and Classification: A Continuing Dispute," Congressional Quarterly Weekly, October 16, 1976, p. 3020; for 1976 see H.R. 8591, H.R. 12006, H.R. 13602, H.R. 15353; for 1977 see News Media Alert, August 1977, which outlines S. 1437 (successor to S. 1), S. 1578, H.R. 89, H.R. 6057, H.R. 6234.

A widely recognized Congressional action concerning penalties for revealing national security information is the codification of the U.S. criminal code. Libertarians throughout the land raised a hue and cry over the so-called "official secrets act" portions of the infamous S. 1 bill.[32] A new version of the bill was introduced in April 1977 by Senators John McClellan and Edward Kennedy. The Criminal Code Reform Act of 1977 (S. 1437 and H.R. 6869) drops the espionage section revisions most offensive to the press.[33]

Both House and Senate have taken steps to include themselves in on at least the declassification of classified information. A permanent Senate Intelligence Committee was created in May 1976; the House formed a similar Committee in July 1977.[34] The 15-member Senate Committee and 13-member House Committee are empowered to study

---

[32] "Opposition to S. 1 Mounts; Bill Called 'Menace to Press'," FoI Digest 17 (July/August 1975):2.

[33] News Media Alert, August 1977, pp. 4, 7.

[34] U.S., Congress, Senate, S. Res. 400, 94th Cong., 2d Sess., 1976; U.S., Congress, House, H. Res. 658, 95th Cong., 1st Sess., 1977.

> the desirability of changing any law, or any Executive order, rule or regulation to improve the protection of intelligence secrets and provide for disclosure of information for which there is no compelling reason for secrecy.[35]

Neither Committee has held hearings yet on secrecy and disclosure.

The establishment of oversight committees represents the Congressional branch's first formal declassification apparatus applicable to the executive classification system. House and Senate versions outline procedures which could result in official release of classified information over the President's objections. In each case, the respective House must vote on the release.

This chapter has briefly outlined Congressional actions in the realm of classification. In search of middle ground between total government secrecy and total disclosure, Congress passed the Freedom of Information Act. After the courts defined the limitations imposed by the first exemption to disclosure in the Act, Congress passed amendments allowing courts to review and release classified information after comparing the classification to criteria

---

[35] S. Res. 400, p. 18.

established by the executive. Thus, it seems Congress has been willing to let the executive control the classification system. The only exception is the Atomic Energy Act in which Congress prescribes controls for atomic information. During the past couple of years, Congressional activity has dealt mainly with formulating legislation to discipline unauthorized disclosure of classified information.

# CHAPTER IX

## CONCLUSION

> Fundamental to our way of life is the belief that when information which properly belongs to the public is systematically withheld by those in power, the people soon become ignorant of their own affairs, distrustful of those who manage them, and--eventually--incapable of determining their own destinies.[1]

President Nixon made that statement upon issuing his executive order to provide classification of national security information. He summed up the problem accurately. A correctly functioning democratic society demands the people's will governs the country, not some secretive president or Congress.

Our fundamental liberties are endangered whenever the secrecy system is abused. Yes, there is an unquestioned need to avoid disclosure of certain sensitive types of information. But when information which should be made available to the people is unnecessarily withheld, our

---

[1] U.S., President, Press statement, Federal Register 37, No. 48, 10 March 1972, 5209.

system is undermined. Information is essential to knowledge and knowledge is the basis for political power.

This study described the rise of the executive secrecy system from strictly military beginnings to a government-wide, seemingly all encompassing information protection system. Problems of administering and overseeing the system were discussed. Rampant overclassification has eroded the validity of the system and made criminal sanctions against those who disclose information almost impossible to administer.

Through the Freedom of Information Act, the courts are empowered, but reluctant, to rule on the appropriateness of a classification. For its part, Congress has acquiesced to an executive system and has only recently provided means to declassify information over the President's objections. Indeed, the whole system itself rests not upon explicit Constitutional authority, but upon implied powers and congressional practical recognition.

What is the solution? David Wise says

> The present classification system should be junked. I doubt there is any need for a formal system of official secrecy in the United States. We only had such a system for a bit more than two decades, and there is nothing in our history that requires its continuation. It is a relic

> of the Cold War. It breeds concealment and mistrust; it encourages the government to lie.[2]

Then he adds, "It is unrealistic, however, to think that Congress and the Executive branch would agree to end all official secrecy." He is probably right.

The ubiquitous William Florence proposes a statutory system which uses the single term "Secret Defense Data."[3] The term would be defined narrowly by Congress and the sole criterion would be probable damage to the national defense. This moves classification back into the strictly military realm from whence it came. Most information would be classified for only three years.

Neither of those solutions has much chance of being accepted. President Carter has proposed a revision of the system to be effective in 1978 which does not radically alter the secrecy system. The biggest proposed change is in the area of sanctions against those who disclose. The Carter draft order includes use of secrecy agreements which the courts have upheld as well within the perview of an

---

[2] Cox, p. 193.

[3] U.S., Congress, Senate, Executive Privilege, Vol. 1, op. cit., pp. 288-92.

agency. Departments will no longer have to threaten their employees with use of the Espionage Act but will be able to prosecute them for breach of contract.

The system continues to exist and be modified. Those who control information intend to continue doing so. The press and the people can only continue to keep chipping away at the edges of the system while recognizing the kernel at the center---a valid need for some secrecy.

# SELECTED BIBLIOGRAPHY

SELECTED BIBLIOGRAPHY

## Books


Barker, Carol M. and Fox, Mathew H. Classified Files: The Yellowing Pages. New York: The Twentieth Century Fund, 1972.

Berger, Raoul. Executive Privilege: A Constitutional Myth. Cambridge: Harvard University Press, 1974.

Cox, Arthur Macy. The Myths of National Security. Boston: Beacon Press, 1975.

Dorsen, Norman and Gillers, Stephen, editors. None of Your Business: Government Secrecy in America. New York: The Viking Press, 1974.

Franck, Thomas M. and Weisband, Edward, editors. Secrecy and Foreign Policy. New York: Oxford University Press, 1974.

Ginger, Ann Fagen, ed. Pentagon Papers Case Collection. Meiklejohn Civil Liberties Institute: Oceana Publications, Inc., 1975.

Mollenhoff, Clark R. Washington Cover-up. New York: Doubleday and Co., Inc., 1962.

Randall, James. Constitutional Problems Under Lincoln. New York: D. Appleton and Co., 1926.

Sheehan, Neil; Smith, Hedrick; Kenworthy, E.W.; Butterfield, Fox. The Pentagon Papers. New York: Quadrangle Books, 1971.

The Senator Gravel Edition/The Pentagon Papers, vol. 1. Boston: Beacon Press, 1971.

Westerman, Sylvia, ed. The CBS News Almanac 1976. Maplewood, N.J.: Hammond Almanac, Inc., 1975.

Wiggins, James Russell. Freedom or Secrecy. New York: Oxford University Press, 1964.

Wise, David. The Politics of Lying. New York: Random House, 1973.

## Law Review Articles

Berger, Raoul. "The Incarnation of Executive Privilege," UCLA Law Review 22 (October 1974):4.

Clark, Elias. "Holding Government Accountable: The Amended Freedom of Information Act." Yale Law Journal 84 (March 1975):741.

"Developments in the Law --- The National Security Interest and Civil Liberties," Harvard Law Review 85 (April 1972):1130.

Diamond, Alan. "Declassification of Sensitive Information: A Comment on Executive Order 11652." George Washington Law Review 41 (July 1973):1052.

Dorsen, Norman and Shattuck, John H.F. "Executive Privilege, the Congress and the Courts." Ohio State Law Journal 35 (1974):12.

Edgar, Harold and Schmidt, Benno C., Jr. "The Espionage Statutes and Publication of Defense Information." Columbia Law Review 73 (May 1973):931.

Gorski, James M. "Access to Information? Exemptions From Disclosure Under the Freedom of Information and the Privacy Act of 1974." Willamette Law Journal 13 (Winter 1976):135.

Henkin, Louis. "The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers." University of Pennsylvania Law Review 120 (December 1971):271.

"National Security and the Amended FOIA." Yale Law Journal 85 (January 1976):401.

"Project --- Government Information and the Right of Citizens." Michigan Law Review 73 (May-June 1975): 971.

Zobrist II, Benedict K. "Reform in the Classification and Declassification of National Security Information: Nixon Executive Order 11652." Iowa Law Review 59 (October 1973):110.

## Public Documents

Act to Amend the Atomic Energy Act of 1946. Statutes at Large, vol. 68 (1954). U.S. Code, vol. 42 (1970).

"Amending the National Security Council Directive of 17 May 1972, Governing the Classification, Downgrading Declassification and Safeguarding of National Security Information." Federal Register 41, 7 October 1976, 45535.

"An Act to Prohibit the Making of Photographs, Sketches, or Maps of Vital Military and Naval Defense Installations and Equipment." Statutes at Large, vol. 52 (1938).

"Armed Forces Industrial Defense and Security Regulations." Federal Register 20, 15 September 1955, 6770.

Crimes and Criminal Procedure. U.S. Code, vol. 18 (1970).

Florence, William G. "Recommendations on Handling Classification Materials," 93rd Cong., 2d Sess., 1972. Congressional Record, vol. 120.

_____. "Important Survey of Secrecy Impact on Government Contractors Under Executive Order 11652," 93rd Cong., 2d Sess., 1974. Congressional Record, vol. 120.

Freedom of Information Act. U.S. Code Annotated, vol. 5 (1977).

"Industrial Personnel Security Clearance Program." Code of Federal Regulations, vol. 32, part 155 (July 1976).

"Information Security Program Regulation." Code of Federal Regulations, vol. 32, part 159 (July 1976).

Interagency Classification Review Committee. 1976 Progress Report. By James B. Rhoads, Acting Chairman. Washington, July 1977.

Internal Security Act of 1950. Statutes at Large, vol. 64 (1950).

"Submission of Reports and Appeals Procedure." Federal Register 42, 13 January 1977, 2679.

Udell, Gilman G., ed. Laws Relating to Espionage, Sabotage, Etc. Washington: U.S. Government Printing Office, 1971.

U.S. Congress. House. Committee on Appropriations. Treasury, Postal Service, and General Government Appropriations for Fiscal Year 1977. Hearings Before a Subcommittee (Part 5), 94th Cong., 2d Sess., 1976.

U.S. Congress. House. Committee on Armed Services. Hearings on the Proper Classification and Handling of Government Information Involving the National Security and H.R. 9853 Before the Special Subcommittee on Intelligence, 92d Cong., 2d Sess., 1972.

U.S. Congress. House. Committee on Government Operations. Availability of Information From Federal Departments and Agencies (Part 8). Hearings Before a Special Subcommittee on Government Information, 85th Cong., 1st Sess., 1957.

_____. Availability of Information From Federal Departments and Agencies (Part 10). Hearings Before a Special Subcommittee on Government Information, 85th Cong., 1st Sess., 1957.

_____. Availability of Information From Federal Departments and Agencies. H. Rept. 1884, 85th Cong., 2d Sess., 1958.

_____. Availability of Information From Federal Departments and Agencies, Progress of Study. H. Rept. 1137, 86th Cong., 1st Sess., 1959.

_____. Availability of Information From Government Departments and Agencies, Progress of Study. H. Rept. 1257, 87th Cong., 1st Sess., 1961.

_____. U.S. Government Information Policies and Practices --- the Pentagon Papers (Part 1). Hearings Before a Subcommittee, 92d Cong., 1st Sess., 1971.

_____. U.S. Government Information Policies and Practices --- the Pentagon Papers (Part 2). Hearings Before a Subcommittee, 92d Cong., 1st Sess., 1971.

_____. U.S. Government Information Policies and Practices --- the Pentagon Papers (Part 3). Hearings Before a Subcommittee, 93rd Cong., 1st Sess., 1971.

_____. U.S. Government Information Policies and Practices --- Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7). Hearings Before a Subcommittee, 92d Cong., 2d Sess., 1972.

_____. Executive Classification of Information --- Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act. Third Report by the Committee on Government Operations, H. Rept. 93-221, 93rd Cong., 1st Sess., 1973.

_____. Availability of Information to Congress. Hearing Before a Subcommittee on H.R. 4938, H.R. 5983, H.R. [illegible]8, 93rd Cong., 1st Sess., 1973.

_____. Security Classification Reform. Hearings Before a Subcommittee on H.R. 12004, 93rd Cong., 2d Sess., 1974.

U.S. Congress. House. Freedom of Information Act Amendments. H. Rept. 93-1380, 93rd Cong., 2d Sess., 1974.

U.S. Congress. House. H. Res. 658, 95th Cong., 1st Sess., 1977.

U.S. Congress. Senate. Annual Report to the Senate of the Select Committee on Intelligence, 95th Cong., 1st Sess., 1977.

U.S. Congress. Senate. Committee on Government Operations. Government Secrecy. Hearings Before the Subcommittee on Intergovernmental Relations on S. 1520, S. 1726, S. 2451, S. 2738, S. 3393, S. 3399, 93rd Cong., 2d Sess., 1974.

_____. Executive Privilege --- Secrecy in Government. Hearings Before the Subcommittee on Intergovernmental Relations on S. 2170, S. 2378, S. 2420, 94th Cong., 1st Sess., 1975.

U.S. Congress. Senate. Committee on Government Operations and the Subcommittees on Separation of Powers and Administrative Practice and Procedure of the Committee on the Judiciary. Executive Privilege, Secrecy in Government, Freedom of Information. Hearings Before the Subcommittee on Intergovernmental Relations on S. 858, S. Con. Res. 30, S.J. Res. 72, S. 1106, S. 1142, S. 1520, S. 1923, S. 2073, vol. 1., 93rd Cong., 1st Sess., 1973.

_____. Executive Privilege, Secrecy in Government, Freedom of Information. Hearings Before the Subcommittee on Intergovernmental Relations on S. 858, S. Con. Res. 30, S.J. Res. 72, S. 1106, S. 1142, S. 1520, S. 1923, S. 2073, vol. III, 93rd Cong., 1st Sess., 1973.

U.S. Congress. Senate. Committee on the Judiciary. Freedom of Information and Secrecy in Government. Hearings Before the Subcommittee on Constitutional Rights on S. 186, 86th Cong., 1st Sess., 1959.

_____. Executive Privilege: The Withholding of Information by the Executive. Hearings Before the Subcommittee on Separation of Powers on S. 1125, 93rd Cong., 1st Sess., 1971.

_____. Freedom of Information Act Source Book: Legislative Materials, Cases, Articles, 93rd Cong., 2d Sess., 1974.

_____. Congressional Access to and Control and Release of Sensitive Government Information. Hearings Before the Subcommittee on Separation of Powers, 94th Cong., 2d Sess., 1976.

U.S. Congress. Senate. "Joint Committee on Atomic Energy Abolishment," 95th Cong., 1st Sess., 1 July 1977. Congressional Record, S. 1185.

U.S. Congress. Senate. Nomination of Theodore C. Sorenson. Hearings Before the Select Committee on Intelligence, 9th Cong., 1st Sess., 1977.

U.S. Congress. Senate. Select Committee to Study Governmental Operations. Supplementary Reports on Intelligence Activities, Book VI. Final Report of the Select Committee to Study Governmental Operations, S. Rept. 94-755, 94th Cong., 2d Sess., 1976.

U.S. Congress. Senate. S. Rept. 2369, 81st Cong., 2d Sess., 1950.

U.S. Congress. Senate. S. 1437. "A Bill to Codify, Revise, and Reform Title 18 of the U.S. Code," 95th Cong., 1st Sess., 1977.

U.S. Congress. Senate. S. Res. 400, 94th Cong., 2d Sess., 1976.

U.S. Constitution, art. 1, sec. 5

U.S. National Security Council. "National Security Council Directive Governing the Classification, Downgrading, Declassification and Safeguarding of National Security Information," Federal Register 37, 19 May 1972, 10053.

U.S. President. Executive Order 8381. Federal Register 5, 26 March 1940, 1145.

_____. Executive Order 10104. Federal Register 15, February 1950, 597.

_____. Executive Order 10290. Federal Register 16, 27 September 1951, 9795.

_____. Executive Order 10501. Federal Register 18, 9 November 1953, 7049.

_____. Executive Order 11652. Federal Register 37, 10 March 1972, 5209.

_____. Executive Order 11905. "United States Foreign Intelligence Activities." Federal Register 41, 1976, 7701.

_____. Title 3, Code of Federal Regulations. 1 January 1949 --- 31 December 1953 Compilation. Washington: U.S. Government Printing Office, 1958.

_____. Title 3, Code of Federal Regulations. 1 January 1959 --- 31 December 1963 Compilation. Washington: U.S. Government Printing Office, 1964.

## Newspapers

Arkansas Gazette, 9 May 1959, p. 6A.

"Carter Aides Draft Secrecy Rules Shift." New York Times, 15 September 1977, p. A18.

"Carter Secrecy Plan Called Worse Than Nixon's." Columbia Daily Tribune, 15 October 1977.

Colby, William. "Modern Intelligence: Myth and Reality." New York Times, 4 August 1975.

Kansas City Star, 21 October 1974.

New York Times, 28 September 1951, p. 30.

New York Times, 5 October 1951, p. 12.

"Reduce Secrecy First." St. Louis Post-Dispatch, editorial, 15 March 1977.

Wall Street Journal, 27 June 1975, p. 1.

Washington Post, 26 September 1951, p. 3.

Washington Post, 18 May 1972.

## Journals/Magazines/Serials

"Army Reveals Long-Classified Secrets." FoI Digest, March/April 1976, p. 6.

Atkins, Jeanni and Boyd, Belvel J. "Classification Reexamined." Freedom of Information Center Report No. 332. Columbia, Mo.: Freedom of Information Center, 1976.

Bagdikian, Ben H. "What Did We Learn?" Columbia Journalism Review, September/October 1971, p. 48.

Blanchard, Robert O. "Present at the Creation: The Media and the Moss Committee." Journalism Quarterly 49 (Summer 1972):272.

"Changes Proposed For Classification System Criticized as 'Weighted Toward Secrecy'." Access Reports 3 (1 November 1977):8.

"Congress Abolishes Joint Committee on Atomic Energy." Congressional Quarterly Weekly Report, 20 August 1977, p. 1752.

"Congress and Classification: A Continuing Dispute." Congressional Quarterly Weekly Report, 16 October 1976, p. 3020.

Cross, Harold F. "The Executive Privilege to Withhold." Freedom of Information Center Report No. 9. Columbia, Mo.: Freedom of Information Center, 1958.

"DOD Outlines Procedures For Access By Historians to Air Force Documents." Access Reports 2 (12 July 1976):8.

"Draft Executive Order Being Circulated Would Revise Classification Procedures." Access Reports 3 (20 September 1977):1.

"FBI Ordered to Produce 15 of 68 Documents Requested by St. Louis Post-Dispatch." Access Reports 3 (28 June 1977):6.

"Federal Judge Rules Government Affidavits Sufficient to Keep Information Classified." Access Reports 2 (4 October 1976):3.

Florence, William G. and Mathews, Ruth. "Executive Secrecy: Two Perspectives." Freedom of Information Center Report No. 336. Columbia, Mo.: Freedom of Information Center, 1976.

Frankel, Max. "The 'State Secrets' Myth." Columbia Journalism Review, September/October 1971, p. 22.

Halperin, Morton. "National Security Information: Congress' Rights." First Principles, February 1976, p. 3.

"In Camera Inspection in FOIA Cases Should Be Limited, Appeals Court Says." Access Reports 3 (11 January 1977):4.

Marwick, Christine M. "Reforming the Intelligence Agencies." First Principles, March 1976, p. 3.

McCartney, James. "What Should Be Secret." Columbia Journalism Review, September/October 1971, p. 41.

Michaelson, Martin. "Up Against the Stone Wall." The Nation, May 1977, p. 614.

News Media Alert. August 1977, pp. 4, 6-11.

"Opposition to S. 1 Mounts: Bill Called 'Menace to Press.'" FoI Digest, July/August 1975, p. 2.

"Protest to Truman Voted on Censorship." Editor and Publisher. 6 October 1951, p. 12.

"Rebuffs at Home, Flak From Abroad." Time, 11 July 1977, pp. 12, 17.

"Security Order." Editor and Publisher, 14 November 1953, p. 44.

"Task Force to Be Formed to Study Classification System." Access Reports 3 (4 May 1977):5.

Taylor, Maxwell D. "The Legitimate Claims of National Security." Foreign Affairs, April 1974, p. 577.

"Text of Judge Gesell's Decision in the Ellsberg Case." New York Times, 25 May 1974.

"Turner: Law May Be Needed to Impede Security Leaks." Congressional Quarterly Weekly Report, 26 March 1977, p. 585.

"Washington Focus." Access Reports 3 (1 June 1977):1.

"When Mr. Truman Sounded Off on Responsibilities of the Press." Editor and Publisher, 13 October 1951, p. 7.

"Where We Stand." Columbia Journalism Review, September/October 1971, p. 27.

Whited, Roberta. "Leaks: Concern and Control." Freedom of Information Center Report No. 356. Columbia, Mo.: Freedom of Information Center, 1976.

## Unpublished Works

Birmingham, Daniel J., Jr. "Problems in the Security Classification System." Maxwell AFB: Air War College, 1975.

Clairborne, Jerry A. "Classified or Declassified." Maxwell AFB: Air Command and Staff College, 1972.

Gangloff, John A. "Safeguarding Defense Information." M.A. thesis, University of Missouri-Columbia, 1971.

Paraschos, Emmanuel. "National Security and the People's Right to Know." Ph.D. dissertation, University of Missouri-Columbia, 1975.

## Cases

Environmental Protection Agency v. Mink, 410 US 73 (1973).

Gorin v. U.S., 312 US 19 (1941).

Halperin v. Dept. of State, 2 Media Law Reporter 2297 (August 1977).

Knopf v. Colby, 509 F2d 1362 (4th Cir., 1975).

New York Times Co. v. U.S., U.S. v. The Washington Post Co. et al., 403 US 713 (1971).

Totten v. U.S., 92 US 105 (1875).

U.S. v. Drummond, 354 F2d 132 (2d Cir., 1965).

U.S. v. Heine, 151 F2d 813 (2d Cir., 1945).

U.S. v. Marchetti, 466 F2d 1309 (4th Cir., 1972).

U.S. v. Nixon, President of the United States, 418 US 683 (1974).

U.S. v. Reynolds, 354 US 1 (1953).

U.S. v. Russo and Ellsberg, No. 9373-(WMB)-CD, District Court--Central District California (1973).

Weissman v. CIA, 2 Media Law Reporter 1276 (1977).

## Miscellaneous

Baron, Gary. Telephone interview. 16 September 1977.

Wells, Robert, Executive Director Interagency Classification Review Committee. Personal letter. 1 September 1977.