

THESIS APPROVAL SHEET

(For use ONLY with an UNCLASSIFIED thesis)

A. STUDENT COMPLETES ITEMS 1 - 7

1. NAME: (b) (3), (b) (6) 2. CLASS NO: NSA - 7
9701
3. THESIS CHAIR: Ms. Anne Brooker-Grogan
4. COMMITTEE MEMBER: (b) (3), (b) (6)
5. THESIS TITLE: Classification Policy: why the United States
Can Not Account for the Cost of Classifying Information
6. THIS THESIS RESPONDS TO A RESEARCH REQUEST FROM A COMMAND OR AGENCY: Yes ___ No X

If Yes, Specify: _____

(If more than one, name all that apply)

7. I understand that this thesis was prepared under the direction of a U.S. Department of Defense institution, and that dissemination outside official U.S. Government channels, either in whole or in part, is prohibited without prior review and clearance for public release as required by DoD Instruction 5330.20.

Signature of Student: _____

(b) (3), (b) (6)

B. COMMITTEE MEMBER COMPLETES ITEM 8

8. THESIS APPROVED: _____ 25 Jul 01
Date

C. THESIS CHAIR COMPLETES ITEMS 9 & 10

9. THESIS APPROVED: _____ 1 AUG 01
Date
10. THESIS MEETS ALL REQUIREMENTS FOR CLEARANCE FOR PUBLIC RELEASE. Yes X No ___ Sign: _____ Date: 1 AUG 01

D. ASSOCIATE DEAN COMPLETES ITEMS 11 & 12

11. DATE PGIP STARTED: Sep 96
12. APPROVAL & AUTHORIZATION TO AWARD THE MSSJ DEGREE: (b) (3), (b) (6) 8/11/01
Date

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government

Distribution (When filled in):

- Original: Bind with thesis
- Copy: Student's File (Registrar's Office)

ABSTRACT

TITLE OF THESIS: Classification Policy: Why the United States Can Not Account for the Cost of Classifying Information

STUDENT:

(b) (3), (b) (6)

CLASS NO.

NSA Cohort 7, Class 9701

Date: August 2001

THESIS COMMITTEE CHAIR: Ms. Arne Brooker-Grogen

THESIS COMMITTEE MEMBER:

(b) (3), (b) (6)

Mankind has pursued intelligence collection since ancient times. The Bible records the Israelites sending spies into Canaan to determine if the land was worth fighting to obtain. Intelligence collection and reporting played an important role in the Battle of Marathon, when the Greeks defeated the Persians because of advanced warning. Most civilizations used spies as well, to obtain and maintain the advantage over their enemies. The Romans and the Chinese knew the value of learning all they could about their adversaries before attacking them, looking for the weakness that could be exploited.

Safeguarding this information is a part of the equation that has largely been ignored. The ancient Greeks were known to shave a man's head, tattoo the information on the man's scalp and then wait for the hair to grow back before sending the messenger back with the information. The hair acted as a classification marking. Similarly, the wax was also used on tablets that had information inscribed on it. The wax was used to cover over the inscriptions and thus safeguard it.

The United States has evolved a classification management system that has grown over time in response to the situations of the day. In other words, the current classification system can be viewed as an ad hoc system that grew out of perceived needs. Adapting a system used by British and French allies during World War I, and modifying it only slightly during that time, the United States has a system that is in need of an overhaul.

Several studies have been conducted of the classification management system, starting with Congressional and Defense Department reviews in the mid-1950s through the late 1990s. All the commissions and committees have said the same thing, that classification is not well

regulated, there is too much of it going on, and a sensible system, grounded in the legal system rather than through Presidential executive order, needs to be implemented.

In the early 1990s Congress mandated that all agencies report their costs of classification management. The first reports were submitted in 1995 and the methodology for such reporting continues to be refined. However, attempting to separate out the costs of classification management is a simplistic approach. What is missed is the larger picture of personnel who are not qualified to handle classified information. Defense Department reports to Congress on its polygraph efforts on applicants, new hires, and current employees are replete with examples of mishandled and compromised classified information. What is the ultimate cost levied by such infractions?

Add to this mix the uncounted costs of pardons given to former government appointees, some of whom were in positions of extremely high trust. The pardon of former CIA DCI Deutch is an example. Mr. Deutch was prepared to plead guilty to charges of neglect when President Clinton pardoned him in January 2001. As a result, no further investigation of what materials Mr. Deutch might have compromised will be conducted and the costs will remain uncounted.

A positive first step towards improving the situation is to make the Security Policy Board a more effective and empowered body. Established in 1994 through President Clinton's Presidential Decision Directive 29, the Board consists of senior executives drawn from across the United States intelligence community. These seasoned veterans should be charged with being more proactive in the oversight arena.

The legislative process needs to be more actively involved. Even though both the House and the Senate have intelligence oversight committees, there is no overarching statute in the United States Code that addresses classification issues. The United States should follow the lead of its partners, the United Kingdom, Canada, Australia and New Zealand, and enact legislation clearly defining what constitutes national security interests. This would then provide the framework to determine what information is truly vital to the nation and merits the cost of safeguarding. It would also be binding on all branches of the federal government, a marked improvement over the current Presidential executive order system, that is binding only on members of the Executive branch.

**CLASSIFICATION POLICY:
WHY THE UNITED STATES CAN NOT ACCOUNT FOR
THE COST OF CLASSIFYING INFORMATION**

by

(b) (3), (b) (6)

National Security Agency
Cohort 7, Class 9701

Unclassified thesis submitted to the Faculty
of the Joint Military Intelligence College
in partial fulfillment of the requirements for the degree of
Master of Science of Strategic Intelligence

August 2001

The views expressed in this paper are those of the author and
do not reflect the official policy or position of the
Department of Defense or the U.S. Government

DEDICATION

A thesis is more than just one person choosing to write about a given topic. It takes family, friends, and advisors to make it happen. I want to acknowledge the countless hours that my reader, (b) (3), (b) (6) spent going over the subject matter with and correcting my work. By extension she too is now a "subject matter expert" on classification costs.

Likewise, my chairperson, Ms. Anne Brooker-Grogan, kept me on the straight and narrow during this project. She never complained about broken promises on my part to get the manuscript to her on time. Another chairperson might well have given up on me as a hopeless cause.

Finally, my wife and daughters have to be acknowledged for their patience and support. Imagine taking a laptop on vacation to get a thesis done! All the same, they tolerated my imposition on their time to get this work done.

To all the women in my life, my chair, my reader, and my family, I dedicate this work. They are free to send me for a psychiatric evaluation if I ever say I want to do something like this again.

(b) (3), (b) (6)

Laurel, Maryland

24 July 2001

PREFACE

Mankind has pursued intelligence collection since ancient times. One of the earliest records in the history of intelligence collection is found in the Bible, with Moses sending members of the tribes of Israel to spy on the inhabitants of the promised-land, Canaan.¹ His intent was to determine the worth of the land; was it worth fighting to obtain? He wanted to know the strength and numbers of the potential enemy; were they going to put up a strong fight to defend this land? This information was used to prosecute the war with the Canaanites, driving them from the land. How much different would the history of the Middle East be if the Israelites had been defeated?

History offers other examples of intelligence used to advantage against an adversary. The Greek messenger Pheidippides, who ran the 26 miles from Athens to Sparta in one day, brought news of the Persian landing at Marathon and sought help from the Spartans. Although the Spartans refused to assist the Athenians, for religious reasons, the Plataeans came to the aid of the Athenians.² The advance notice given to the Athenians, provided by intelligence on the strength and disposition of the Persians, furnished information crucial to the successful prosecution of the war by the Greeks against the Persians. History would no doubt be much different today if the Persians had succeeded. The Greeks, instead of flourishing in the Mediterranean, would have been subsumed by Persian culture. A subsequent Roman conquest of Greece, if such a thing

¹ The Bible, Deuteronomy, Chapter 1, Verses 20-25.

² Herodotus, *The Histories* (Baltimore Md.: Penguin Books Ltd., 1964), 398-400.

were to have happened, would have resulted in a very different cultural attitude. In turn, Western Europe would have had a very different legal and cultural standard.

The ancient Romans used spies as well, often disguised as ordinary peasants, artisans, and exiles.³ They were able to infiltrate areas that noble or highborn Romans could not easily access without attracting attention. Information obtained from hostile areas was then passed on for use by the kings, then by the consuls during the Republic, and finally by the emperors and their councils during the Empire period. The successful, quiet acquisition of this information enabled Rome to last for many centuries.

The use of intelligence was known and appreciated outside of the European and Middle Eastern arenas as well. Sun-Tzu advises the reader to know the terrain and know the field of battle.⁴ He decrees that the good general will “determine (the enemy’s) disposition of force to know the tenable and fatal terrain.”⁵ This clearly requires gathering intelligence on the enemy and the battlefield, before going to battle, to successfully win the day.

In each instance the information was obtained without fanfare and without any announced intentions. People in positions of power used this surreptitiously obtained information to make informed decisions. The source of the information was hidden to preserve confidentiality. The practice of obtaining information through hidden or secret means, and passing it on for further use continues today as spying. Much has been

³ Levy, *The Early History of Rome* (Baltimore Md.: Penguin Books, Ltd., 1967), 76.

⁴ Sun-Tzu, “The Art of War,” *The Seven Military Classics of Ancient China*, translator Ralph D. Sawyer (Boulder Co: Westview Press Inc, 1993), 167.

⁵ Sun-Tzu, 168.

written about the profession of spying, referred to by some as the second oldest profession in history. But the other half of the equation - how to safeguard the information that an enemy would find of value - has largely been ignored.

This paper will examine the way in which the United States Government has developed its present policy of classifying information deemed worthy of protection from enemy eyes. In addition, this paper will address how the system evolved, its strengths and weaknesses, and what the annual cost to the population at large was estimated to be in the recent past, with the establishment of a cost accounting system.

Our system is regulated by a series of presidential executive orders rather than through the legal code. In addition, executive orders are not viewed as binding on either the Legislative or Judiciary branches of the Federal Government – only the Executive branch and its employees. To compound the problem, new orders are promulgated that do not clearly cancel earlier orders, leaving room for confusion and doubt among those workers bound by those orders – the federal workers in the Executive branch. Because our system lacks legislation that clearly defines what constitutes classified material and spells out the consequences of mishandling or disclosing such material, it is open to abuse and misuse. The Presidential pardon of John Deutch by President Clinton illustrates what can happen when someone who has mishandled classified information is not properly punished. The precedent set often leads to more abuse.

Once the information has been obtained, it has to be safeguarded in some fashion. The material must be clearly labeled as sensitive. The British, through their Official Secrets Acts, provide clear guidance regarding what is deemed secret and what steps are needed to protect the information.

The United States, in contrast, did not approach this issue until the outbreak of World War II. Prior to that time, each agency and department responsible for intelligence gathering protected the information as it saw fit. A uniform classification system, outlining levels of sensitivity and providing explanations, was not adopted until after World War II, when the Eisenhower Administration issued Executive Order 10501 in November 1953. This order continued in effect, relatively unchanged, for the next twenty years. Although subsequent Executive Orders have been issued, none is viewed as being binding as a law.

This thesis, drawing from unclassified sources, will examine the evolution of classification. This will include an examination of the early years of the Republic, when the Alien and Sedition Acts of 1798 were enacted, to the end of the 20th century. Several commissions and committees have examined the question of classification questions and this thesis will look at the results of those inquiries. Finally, an examination of how the government currently calculates the costs of classifying material will be made and a determination of whether or not this methodology is flawed and why will be presented.

CONTENTS

Preface.....	iii
List of Tables.....	viii
Chapter	Page
CHAPTER 1: A BRIEF REVIEW.....	1
The Revolutionary War and The Early Years of the Republic, 1	
The Civil War Era, 6	
The Post Civil War Era to World War I, 8	
World Wars I and II, 9	
Other Agencies, 10	
The Legislative Branch and Intelligence, 10	
The Judiciary, 14	
The Executive Branch and Intelligence, 15	
Our English Speaking Partners and Their Legislation, 17	
CHAPTER 2: INVESTIGATIVE STUDIES.....	21
The 1950s – The First Examinations, 21	
The 1960s – Concerns Continue, 22	
The 1970s – Time of Major Changes, 24	
The 1980s – Halting Steps, 26	
The 1990s – Studies and Commissions Continue, 29	
CHAPTER 3: GETTING A HANDLE ON CLASSIFICATION	38
The ICRC – Trying to Put the Genie in the Bottle, 38	
The ISOO – Continuing the Work, 42	
CHAPTER 4: PUTTING A PRICE ON THE COST OF CLASSIFICATION.....	56
Dollar Amounts, 56	
Polygraphs – Another Form of Classification Management, 62	
CHAPTER 5: WHY IT DOES NOT ADD UP.....	65
The Need for Accounting, 65	
How to Undermine the Situation, 65	
Some Suggested Solutions, 67	
Bibliography.....	70

LIST OF TABLES

Table	Page
1. Presidential Executive Orders.....	17
2. Review Committees.....	37
3. Original Classification Authorities from 1971 to 1977.....	39
4. Original Classification Decisions from 1973 to 1977.....	41
5. Original Classification Authorities from 1979 to 1989.....	44
6. Derivative Classifiers Government-wide in 1979.....	45
7. Original Classification Decisions 1979 to 1981.....	45
8. Derivative Classification Decisions 1979 to 1981.....	46
9. Original Classification Decisions 1982 to 1989.....	48
10. Derivative Classification Decisions 1982 to 1989.....	49
11. Ratio of Original to Derivative Classification Decisions in the 1980s.....	50
12. Original Classification Authorities 1990 to 1999.....	51
13. Original Classification Decisions 1990 to 1999.....	52
14. Derivative Classification Decisions 1990 to 1999.....	53
15. Ratio of Original to Derivative Classification Decisions during the 1990s.....	54
16. Government and Industry Classification Costs 1995 to 1999.....	57
17. Estimated Government Classification Costs by Category – 1995 to 1999.....	58
18. Information Security Cost Estimates 1995 to 1999.....	59
19. Information Security Costs as Percentages of Dollars Spent – FY 1995.....	59
20. Information Security Costs as Percentages of Dollars Spent - FY 1996.....	60
21. Information Security Costs as Percentages of Dollars Spent - FY 1997.....	60
22. Information Security Costs as Percentages of Dollars Spent - FY 1998.....	61
23. Information Security Costs as Percentages of Dollars Spent - FY 1999.....	61

CHAPTER 1

A BRIEF REVIEW

THE REVOLUTIONARY WAR AND THE EARLY YEARS OF THE REPUBLIC

The United States has historically had an aversion to holding any information in secret, associating it with “privilege and sinister maneuvering, both of which go against the grain.”¹ This is explained, in part, by the fact that during the United States’ colonial era the British proved to be expert at using spies. Colonists were routinely denounced by spies of all types and often were not afforded the opportunity to face their accuser.² A casual remark to an acquaintance or close friend could lead to condemnation and arrest. Combined with the powers granted to the governors who were appointed by the Crown to act as they saw fit, the British left the former colonists with an aversion of anything done in secret.

Some of the founding fathers, such as Thomas Jefferson and James Madison, were opposed to any form of secrecy. Others, such as Alexander Hamilton and Benjamin Franklin, were more pragmatic. The proceedings for the Continental Congress of the United Colonies, which drafted the Declaration of Independence, were kept secret during

¹ Edward F. Sayle, “The Historical Underpinnings of the U.S. Intelligence Community,” *The International Journal of Intelligence and Counterintelligence* 1, no. 1 (Spring 1986): 1.

² G.J.A. O’Toole, *Honorable Treachery: A History of U.S. Intelligence Espionage and Covert Action From the American Revolution to the CIA* (New York: The Atlantic Monthly Press, 1991), 10-11.

the deliberation stages.³ In fact, the precedence was established at the outset when, in 1775, "... the Continental Congress began to meet regularly following the skirmishes at Lexington and Concord, the members imposed a resolution of strict secrecy on themselves."⁴ The same was true for the conventions that drafted the Articles of Confederation and, later, the Constitution of the United States. Both the Articles of Confederation⁵ and the Constitution⁶ include provisions to keep those deliberations made by Congress, deemed to be sensitive governmental matters, out of the public record so long as those deliberations are considered sensitive. The Articles of Confederation, which came into effect as the governing document for the United States in 1781, provided for legislative secrecy under Article IX. It is important to remember that the Articles of Confederation did not establish an executive branch. At that time, the president did not head up a branch of government, as he would under the Constitution, but was the head of the Congress. Thus, the authority for secrecy matters rested with the Congress during that time.

An important outgrowth from the experience with the Articles of Confederation was the insistence on amending the Constitution immediately with The Bill of Rights. The Bill of Rights, the first ten amendments to the United States Constitution, was included because of fears of government abuse of power. Since the Constitution granted

³ Arvin S. Quist, *Security Classification of Information*, Vol. 1, on-line edition (Oak Ridge National Laboratory, 1989), URL: <<http://www.fas.org/sgp/library/quist/index.html>>, accessed 14 March 2001.

⁴ Scott D. Breckenridge, *The CIA and the U.S. Intelligence System* (Boulder, CO: Westview Press, Inc, 1986), 89.

⁵ *United States Articles of Confederation*, art. IX.

⁶ *United States Constitution*, art.1, sec. 5.

more power to the federal government than had been afforded it under the Articles of Confederation, The Bill of Rights was written to ensure that the citizenry would not have its rights and liberties curtailed by the government in power.⁷ Implied in this was freedom from spying.

The founders of this nation started out with a healthy skepticism about those in power. They believed that a temptation existed for those in power to seek to maintain their authority by whatever means at their disposal. Hence, they saw the need to design within the government a system of checks and balances. ... The framers clearly intended that these procedures and limits would apply even when the government was invoking what we now label its "national security" powers.⁸

Congress established the Committee of Secret Correspondence during the Revolutionary War. This organization, which can be viewed as the first intelligence agency, "...withheld from the Continental Congress many of the details of its sensitive negotiations with France, explaining, 'We find by fatal experience, the Congress consists of too many members to keep secrets.'"⁹ When Congress discovered that Thomas Paine, the secretary for the Committee of Secret Correspondence, had divulged information from the committee's files it attempted to take further action. Since the Committee of Secret Correspondence had been communicating with sympathizers in England and Ireland, it could not be determined if Paine had been intentionally spying or simply indiscreet. There were no espionage laws in effect at that time, so Paine could not be punished. "To remedy this situation, the Congress appointed a Committee on Spies,

⁷ Morton H. Halperin, "Intelligence in an Open Society," in *Intelligence – Policy and Process*, eds. Alfred C. Mauer, Marion David Tunstall and James M. Keagle (Boulder CO: Westview Press, 1985), 101.

⁸ Halperin, 101.

⁹ O'Toole, 96.

which revised the Articles of War to make treason punishable by death.”¹⁰ Congress passed the Alien and Sedition Acts¹¹ in July 1798 in anticipation of war with France. The Act was opposed by the anti-Federalists, such as Jefferson and Madison and was allowed to expire in the 1800s, once the anti-Federalists came into power. The next time such legislation would be enacted would be over one hundred years later, with passage of the Espionage Act of 1917.¹²

It was recognized that business in the government would, on occasion, be extremely sensitive and as such merited special considerations and safeguards. Under the Articles of Confederation, this meant that ultimately Congress was responsible. Later, when the Constitution was adopted, the Executive branch was instituted. The president was given, under Article II, Section 2, the power to make treaties, pending Senate approval. The apparent intent was to ensure that the “...Commander in Chief’s ability to defend American interests (not) be impeded by the endless congressional delays and leaks which bedeviled George Washington during the Revolutionary War.”¹³

Although he originally opposed the need to replace the Articles of Confederation with the Constitution, Thomas Jefferson later wrote, “The transaction of business with foreign nations is executive altogether...” “Thus, all foreign-affairs matters beyond treaty-making, including foreign intelligence activities, were deemed literally to be none

¹⁰ Breckinridge, 89.

¹¹ Seymour Martin Lipset, “George Washington and the Founding of Democracy,” *Journal of Democracy* 9, no. 4 (October 1998): 27.

¹² Daniel Patrick Moynihan, *Secrecy* (New Haven CT: Yale Press, 1998), 84-85.

¹³ Stephen Knott, “Executive Power and the Control of American Intelligence,” *Intelligence and National Security* 13, no. 2 (Summer 1998): 171.

of the Senate's business and could be properly conducted under a cloak of secrecy when the president felt it necessary to do so."¹⁴

While the Constitution addressed the need for secrecy in the Legislative branch it did not address the need for secrecy in the Executive branch. However, Congress allowed the president to have discretionary funds and secret missions were funded from these monies. In the early days, "...intelligence was conducted on a highly personal and private basis by talented amateurs responsible solely to the President."¹⁵

A nascent intelligence community in America began with the administration of George Washington. Soon after he became president, Washington asked Congress for a "competent fund," a request that Congress both understood and granted – with minimal unseemly public debate. On July 1, 1790, it gave the president a "contingent fund of foreign intercourse," known as the secret service fund for what would now be called human intelligence activities and covert action. Washington accounted for this fund by simple certificate. ... By 1792 Washington's secret service fund had risen to \$1 million – about 12 percent of the total U.S. budget.¹⁶

During the Revolutionary War, President Washington, as the then General of the Continental Army, ran a successful spy network against the British. During his presidential terms Washington ran an extensive spy network in Europe, paying these people from his discretionary funds.

Over time the Executive branch devised a marking system for sensitive materials.

During the Madison administration intelligence and other government secrets gained the added protection of formal document classification; "secret," "confidential," and "private." A fourth level was not added until

¹⁴ O'Toole, 96.

¹⁵ Sayles, 1.

¹⁶ George A. Carver Jr., "Intelligence in the Age of Glasnost," *Foreign Affairs* 69, no. 3 (Summer 1990): 148-149.

World War I, when “top secret” was created to contend with “most secret” information received from Britain.¹⁷

During this time, however, no legislation was enacted to recognize either the confidential matter of the president’s discretionary fund, or to recognize and standardize the classification scheme introduced by the Madison administration. Each agency was free to classify information as it deemed appropriate; materials marked “private” by one agency might be marked “secret” or “confidential” or left unmarked by another agency. With regards to the president’s discretionary fund, Congress asked President Polk to surrender the accounts for the contingency fund under the Tyler administration. President Polk refused and Congress retaliated by discontinuing the fund.¹⁸

THE CIVIL WAR ERA

With the advent of the Civil War, both the Union and Confederate sides saw the need to obtain as much information on each other as possible and employed spies and spying techniques, also referred to as tradecraft, to further their causes. During this time innovations such as the telegraph for long distance communications and aerial photography were used, as well as the more traditional human spy. Innovative ideas and techniques were required to exploit the information. Too often the value of the information was not appreciated, and proper safeguards were not employed. In some cases, information was underutilized or not used at all. In addition, valuable information was often compromised because proper safeguards were not in place; for example,

¹⁷ Sayles, 10-11.

¹⁸ Sayles, 15.

telegraph lines were often tapped for the information they contained. Messages were sent either unencoded or in very weak codes that were easy to break. Balloons were used by aerial observers to watch and photograph activity behind enemy lines.¹⁹ Often the aerial observers could discern armed strength, troop deployments, and the level of supplies available to the forces on the front line. Camouflage techniques were not used effectively. Finally, the Confederates had a formal structure in place during the Civil War for intelligence gathering, carried out by the Signal and Secret Service Bureau, located in the War Department.²⁰

The press played a decisive role as well.²¹ Often Union troop movements were reported in the Northern press before the soldiers had begun to move. This advance notice enabled the Southern forces to prepare for the encounter and defeat the Northern forces. In contrast, the Southern press honored the press-censorship placed on it and denied the Northern forces valuable information.²² Compounding the fact that no legislation restricted the flow of sensitive information to the press, no guidelines existed clarifying what was sensitive information and what was not. As a result of this oversight, the North suffered in the early days of the war, losing several battles to an enemy inferior in number but superior in the use and exploitation of intelligence. It required a tremendous effort to control the free flow of information and categorize what constituted

¹⁹ O'Toole, 133.

²⁰ O'Toole, 128-130.

²¹ O'Toole, 131.

²² O'Toole, 131-132.

sensitive information.²³ By the end of the Civil War, efforts were underway to standardize methods of categorizing and safeguarding information.

THE POST CIVIL WAR ERA TO WORLD WAR I

However, these efforts were short-lived. Following the end of the Civil War, the machinery used to classify information was dismantled and forgotten. When the United States Navy established the Office of Naval Intelligence (ONI) in 1882, and the United States Army re-established its intelligence service in 1885, they did so in complete independence of one another; neither service communicated directly with the other on intelligence matters. Each service established its respective intelligence service with the purpose of gathering information on technology; that is, the focus was on technology transfer and not on gathering what would be categorized as intelligence data on potential adversaries.²⁴ Although each service sent military attaches abroad to serve as observers and intelligence collectors, neither service shared its findings with the other, even when the information may have proved useful to the other. In addition, no formal structure for classifying, storing, and sharing secrets was actually established; each service marked and protected the information it gathered inconsistently. What one service considered important and worth safeguarding often was not viewed in the same fashion by the other service. This situation continued through the various wars in Europe and the Pacific during the late 19th and early 20th centuries.

²³ O'Toole, 172-173.

²⁴ O'Toole, 180.

WORLD WARS I AND II

The United States Army came under the tutelage of the British and French intelligence services during World War I and adopted many of the practices and structures used by them.²⁵ Meanwhile, the United States Navy came under the wing of British Naval intelligence, but had an extremely limited role to play and was not included to the same extent as the Army had been.²⁶ As a result, each service learned different lessons.

One lesson neither service learned was how information was shared by the British military structure; i.e., the British Army and Navy routinely shared information with one another. This practice of not sharing information continued into the 1940s.²⁷ Despite the disastrous effects of Pearl Harbor in 1941, the Army and Navy continued their rivalry with each other throughout the war as evidenced by the PURPLE intelligence. PURPLE was encoded Japanese information that gave the US military a window into the thinking and planning of the Japanese. Because of their rivalry, the Navy and the Army alternated days for decrypting and reporting PURPLE intercept. This resulted in incomplete intelligence reporting, with each service possessing only a portion of the overall intelligence picture.²⁸ The rivalry moderated to some degree in the latter half of World War II when it was recognized that a joint effort was needed to end the war. While a certain amount of rivalry continued after World War II, it was greatly diminished during

²⁵ David Kahn, *The Codebreakers* (New York: MacMillian Publishing Co, 1967), 354.

²⁶ Kahn, 387.

²⁷ Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford CA, Stanford University Press, 1962), 97.

²⁸ Wohlstetter, 109.

the Cold War when both services realized that neither could successfully carry out its Cold War mission without the assistance of the other.

OTHER AGENCIES

Throughout the 19th and 20th centuries, the United States State Department conducted its own intelligence gathering operations separately from the military intelligence operations. As a consequence, State Department information that may have had an impact on the Army or the Navy was not routinely shared with either branch of the military. Other agencies, e.g., the United States Coast Guard, which was part of the Treasury Department until 1967 at which time it was transferred to the Department of Transportation, and the Federal Bureau of Investigation (FBI) under the Justice Department, required secrecy in order to operate effectively. Yet each organization pursued its own interests and goals independently and those goals were not always compatible with the goals and aims of other United States Government organizations. In fact, sometimes the law was totally ignored when deemed necessary to complete its mission.²⁹

THE LEGISLATIVE BRANCH AND INTELLIGENCE

As mentioned earlier, there was no legislation enacted by Congress that standardized and codified what constituted sensitive information. There was, however, legislation that dealt with standards of conduct for personnel. The Espionage Act of 1917, enacted during World War I, defined what constituted a criminal offense with

²⁹ Wohlstetter, 39.

regard to damaging U.S. national security during time of war. The Sedition Act of 1918 went on to define what constituted a criminal offense, i.e., actively seeking to damage the interests of the United States by any agent of a foreign power. Both Acts stopped short at imposing censorship since that was viewed as a violation of the First Amendment.

The Espionage Act of 1917 can be viewed as the direct successor to the Aliens and Sedition Act of 1794. The Sedition Act of 1918 was repealed in 1921 while the Espionage Act of 1917 was allowed to remain in force. The Espionage Act of 1917 was amended twice, once in 1933 and again in 1938. The 1933 amendment made it a criminal offense for a federal employee to sell any codes to a foreign power. The 1938 amendment made it a criminal offense to photograph military installations.

Despite the Espionage Act, “Presidents Wilson and Hoover and Secretaries of State Kellogg and Stimson advocated increased openness, honesty, and trust in government.”³⁰ The story of Herbert O. Yardley and the Black Chamber from the 1920s has been written about and discussed in a variety of texts. During Yardley’s time in the Black Chamber every effort was made to hold employees to the Black Chamber’s cover story and adhere to its security policies.³¹ The fact that Secretary of State Stimson closed the Black Chamber’s activity in 1928 led Yardley to later write a book about his experiences. He also sold his services to various foreign powers in order to make a

³⁰ Robert G. Angevine, “Gentlemen Do Read Each Other’s Mail: American Intelligence in the Interwar Era,” *Intelligence and National Security* 7, no. 2 (1992): 23.

³¹ James Bamford, *The Puzzle Palace: A Report on America’s Most Secret Agency* (Boston, MA, Houghton Mifflin Co., 1982), 8-9.

living. This led to the first amendment of the Espionage Act of 1917, passed in 1933, which prohibited federal employees “from publishing any foreign code or anything transmitted in such a code.”³²

Hatton W. Summers, a Texas Democrat and chairman of the House Judiciary Committee, introduced legislation to protect government documents in Congress on March 7, 1933. The bill, *For The Protection of Government Records, H.R. 4220* “... made it a crime for any government employee to ‘sell, furnish to another, publish, or offer for sale’ any government document, regardless of whether it was classified or dealt with any subject relating to codes, just so long as the release of information could be shown to be ‘prejudicial to the safety or interest of the United States.’”³³ President Franklin Roosevelt signed H.R. 4220 on June 10, 1933. As Public Law 37, the statute provided for a fine of \$10,000.00 or a prison term of 10 years or both for willful, unauthorized disclosure of any official United States diplomatic codes and any material prepared using such codes. The law remains a part of the criminal statutes with only minor changes. It has since become part of Section 952 of Title 18 of the United States Code.³⁴

With this as a backdrop there was a suspicion of government secrecy. The Radio Act of 1927 was designed to protect the populace against government snooping.³⁵ Prior to this Act, law enforcement was free to listen in to telephone conversations or “tap” communications. Treasury officials, during Prohibition, routinely monitored radio

³² Moynihan, 97.

³³ Bamford, 25.

³⁴ Bamford, 26.

³⁵ Angevine, 23.

transmissions from smugglers bringing alcohol from Canada and Mexico. The Act established that there could not be an expectation of privacy when using the public airwaves, since the airwaves are available for anyone with the proper transmission and reception equipment to use. However, telephone conversations in the newly-networked nation were then carried on copper wire, using equipment owned and operated by the telephone company, a private entity. Since the calls were not broadcast over the public airwaves, but on privately owned equipment, there was an assumption of privacy. The Radio Act of 1927, therefore, required judicial sanctioning for “tapping” the telephone wires. This was viewed as enforcing the Fourth Amendment, which guarantees against unwarranted search and seizures.

The Nye Commission of 1934 represented the height of suspicion of any governmental monitoring or “secret” activities.³⁶ Named for Senator Nye of New York, the Commission called into question the need for the Espionage Act, since it was viewed as a threat to freedom of speech, while the Commission looked at strengthening the Radio Act of 1927. The Federal Communications Act of 1934 was a direct result of the Commission’s work. Clearly the Congress was split on the issue of sensitive intelligence matters, as witnessed by the legislation passed.

Congress passed the Nuclear Energy Acts of 1948 and 1954. The first Act established the Atomic Energy Commission and defined what constituted classified information. The second Act superceded the first, refining and better defining the law as enumerated in the first Act. This represents the only attempts by Congress to govern classified information legislatively. The argument used in establishing classification for

³⁶ Angevine, 23.

nuclear information was that some information was “born classified” and merited immediate protection. This concern began in the late 1930s, when scientists and academics working on nuclear research were concerned about reports of Nazi efforts to develop a nuclear device. The concern continued following the end of World War II, when relations with the Soviet Union deteriorated, and a fear existed that nuclear-related information could be used to change the balance of power in the world. Although several attempts have been made to pass legislation governing other forms of classified information, Congress has never passed any other such legislation.

THE JUDICIARY

The United States legal system has essentially remained separate from the issues of national security, i.e., sensitive and classified information and the processes that the legislative and executive branches employed to implement statutes and executive orders to address national security needs. The precedent was set early on when the Supreme Court did not rule on the constitutionality of either the Espionage Act of 1917 or the Sedition Act of 1918 until after World War I had ended. “The enduring legal precedent established by the Court in its consideration of these acts comes from *Schenck v. United States*. In writing the opinion on behalf of the Court, Justice Oliver Wendell Holmes articulated the test of ‘clear and present danger.’ The ruling affirmed that Congress has the right to limit speech in an attempt to limit certain ‘evils.’”³⁷

³⁷ Moynihan, 108.

THE EXECUTIVE BRANCH AND INTELLIGENCE

The Franklin D. Roosevelt Administration issued Executive Order 9066 in February 1942. Citing the Espionage Act of 1917 as amended, this executive order expanded on the prohibition against photographing military installations by giving the Secretary of War the authority to exclude persons from designated areas in order to afford protection of those areas from sabotage and espionage. Other executive orders under the Roosevelt and Truman administrations covered such issues as the establishment of the Office of Strategic Services (forerunner to the Central Intelligence Agency), the establishment of the Director of Central Intelligence position, and the categorization of sensitive information.

The Eisenhower administration, in November 1953, issued Executive Order 10501 that refined and clarified classification levels. Importantly, the executive order, rather than citing the Espionage Act of 1917, references the president's authority as coming from Article II of the Constitution. This claim continues to be made to this day.

The Eisenhower executive order remained in force for approximately 20 years, with only some modifications made by the Kennedy Executive Order 10964. President Nixon's order repealed both prior orders in 1972, issuing new guidance. The Carter administration issued Executive Order 12065 shortly after taking office in 1976, canceling the Nixon executive order. It restricted the terms for classification and imposed short time limits for keeping information classified.

The Reagan administration, shortly after coming into office, canceled the Carter order. Executive Order 12356 changed the time limit to an indefinite period of time.

This, combined with the requirement to obtain permission from the originating agency to declassify information, has hindered the current declassification efforts.

The Clinton administration issued Executive Order 12958 in April 1995, establishing nine categories of classified information and setting a 25-year time limit. At the same time, the order mandated automatic declassification of any information over 25 years old by the end of the year 2000 – a requirement that has since been modified due to difficulties in meeting that goal. A subsequent executive order established the guidelines for issuing clearances to permit access to classified information. The accompanying table highlights the major points of each of the executive orders. Note that oversight has not been consistently addressed through the post World War II era. Likewise, portion marking of paragraphs, a useful tool in determining what portions of a document can be declassified, was not mandated until the Nixon era, approximately 25 years into the Cold War period.

Each president has issued his own executive order as a way to place his “personal stamp” on the issue of classification. The executive order system evolved in what can be viewed as an arbitrary manner. From citing an existing statute to citing the Constitution, the executive order system is afforded the weight and credibility of law, when in fact no such authority is explicitly granted by the Constitution. It is only by interpretation of Article II of the Constitution, which grants the president control over national security, that this authority is claimed. Since the executive orders are not statutes, they are not viewed as binding on the legislative or judiciary branches.

PRESIDENT	EISENHOWER	KENNEDY	NIXON	CARTER	REAGAN	CLINTON
EXECUTIVE ORDER	10501	10964	11652	12065	12356	12958
YEAR ISSUED	1952	1962	1972	1976	1982	1995
Declassification date or event on document at time of classification	YES	YES	YES	YES	OPTIONAL	YES
Portion marking of paragraphs in a document	NO	NO	YES	YES	YES	YES
Balancing test of the public's right to know and need to protect	NO	NO	NO	YES	NO	NO
Appeals or oversight structure	YES	NO	YES	YES	YES	YES
Scheduled automatic declassification review or release	NO	YES	YES	YES	NO	YES
Formal mandatory review procedures	NO	NO	YES	YES	YES	YES

Table 1 – Presidential Executive Orders

Source: Author created

OUR ENGLISH SPEAKING PARTNERS AND THEIR LEGISLATION

The United States has had an intelligence sharing arrangement of one sort or another with the United Kingdom, i.e., Great Britain, since World War I. As mentioned previously, the United States modified its classification system, adopting the classification system used by the British and French. It bears noting that the French have not been primary partners since World War I. They routinely keep their intelligence documents classified for at least sixty years from date of classification.³⁸

³⁸ Douglas Porch, *The French Secret Services* (New York: Farrar, Straus, and Giroux, 1995), XII.

“The protection of shared information is greatly assisted by the acceptance of a common system of security classifications and codewords throughout the UKUSA countries.”³⁹ This system continues to the present day.

Compartmentalization and the “need-to-know” principle are applied on the basis of the source of the material, the method of collection, and the particular needs of those requiring access to the information. ... In the case of SIGINT [signals intelligence] material or Special Intelligence [SI], the series of codewords derive directly from the system accepted under the BRUSA [Britain-US] Agreement of 17 May 1943...”⁴⁰

The British instituted a legislative system to control sensitive information in the late 19th century with the passage of the first Official Secrets Act in 1889. The Act was modified in 1911 and again in 1989 and 1994. The Acts clearly define what is considered sensitive information and how it is to be safeguarded. The Official Secrets Act of 1889 was instituted because “... the increasing bureaucratization and size of the state in the U.K. (United Kingdom) produced a fresh concern for the security of the state’s information...”⁴¹ The Acts were introduced in and approved by the Parliament and are part of the national legal system. The Prime Minister, while heading what could be termed the British executive branch, is a sitting member of Parliament and represents a district in the House of Commons. He is chosen by his party membership and not by the populace. There is no head of government similar to the United States president, elected to office without representing a district in Congress. Therefore, the mechanism for executive orders is not there.

³⁹ Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind*, 2nd Ed. (Cambridge, MA: Unwin Hyman Inc., 1990), 164.

⁴⁰ Richelson and Ball, 166.

⁴¹ Peter Gill, “Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community,” *Intelligence and National Security* 11, no. 2 (April 1996): 315.

Canada, Australia, and New Zealand, as members of the British Commonwealth, have followed the British lead on several of these issues. All three nations adopted the parliamentary form of government. All three relied on the British Official Secrets Acts to serve as a model.

Recently, each has begun to rewrite legislation to suit its particular needs. The British Official Secrets Act has been criticized as being overly restrictive. As Andrew Christopher has written, “British taboos are, by tradition, bigger and better than their American counterparts; nowhere is this truer than in the field of intelligence.”⁴² Canada, Australia, and New Zealand, as nations developing their own traditions and needs, are redefining their legislation to suit their needs. New Zealand, for example, introduced the Official Information Act in 1982. The new Act increases accountability, promotes effective participation and “...protect(s) official information to the extent consistent with the public interest...”⁴³ Australia has also changed its intelligence legislation to respond to its particular needs. Since 1976, when the government of Prime Minister Gough Whitlam was voted out of office, legislative steps have been taken to conduct its intelligence business “with circumspection under a system of sensible and democratic controls.”⁴⁴

The British model, because it provides a clear definition of what does and does not constitute a secret, represents an enabler that, if used properly, would permit fairly accurate cost estimates for classifying information. Also provided would be the cost of

⁴² Andrew Christopher, “Historical Research on the British Intelligence Community,” *Comparing Foreign Intelligence – the US, the USSR, the UK, and the Third World*, ed. Roy Gibson (McLean, VA, Pergamon – Brassey’s International Defense Publications, 1987), 43.

⁴³ Nicky Hager, *Secret Powers: New Zealand’s Role in the International Spy Network* (Nelson, NZ, Craig Potton Publishing, 1996), 231-232.

⁴⁴ Harvey Barnett, “Legislation-based National Security Services: Australia,” *Intelligence and National Security* 9, no. 2 (April 1994): 299.

maintaining that information in a secure environment, as well as an estimate of what the cost would be to declassify information, both in terms of costs spent in the declassification process and costs to the national security if the information were made public.

CHAPTER 2

INVESTIGATIVE STUDIES

THE 1950s – THE FIRST EXAMINATIONS

Beginning with the Eisenhower administration and continuing into the late 1990s, several studies on classification and security issues have been conducted at the request of both Congress and the Executive branch. Secretary of Defense Charles E. Wilson established the five member Committee on Classified Information in August 1956. Charles A. Coolidge, a former assistant secretary of defense, chaired the committee.

Three months after it was set up, on November 8, 1956, the Coolidge committee issued a report containing twenty-eight recommendations – ten covering overclassification, eleven relating to unauthorized disclosures of information, and the remaining seven relating to department policies vis-à-vis Congress, industry, and the press. The first recommendation – based on a finding that Defense Department officials had a tendency to “play it safe” and classify too much – called for “a determined attack” on overclassification.⁴⁵

During this time Congress was also looking at classification issues. The “Moss Subcommittee – Special Government Information Subcommittee,” was established in 1955 to monitor executive secrecy. The subcommittee examined overclassification, its administration, and the lack of accountability. While disciplinary action resulted from not classifying information, conversely, none existed for information classified that

⁴⁵ Moynihan, 171.

should not have been.⁴⁶ This finding, as noted by the Coolidge-led committee, led to extreme caution. As an outgrowth of the Moss subcommittee, focus continued on the rights of Congress and the public to obtain information, whether classified or not, from the executive branch. The Freedom of Information Act of 1967 was a direct result of the subcommittee's work.

On January 18, 1955, Senators John C. Stennis and Hubert H. Humphrey introduced Senate Joint Resolution 21, an act to establish the Commission on Government Security.” They echoed the concerns that classification could be used as a means of covering abuse and mistakes. “*The Report of the Commission on Government Security*, published in June 1957, ... was encyclopedic and fair-minded. ... (H)owever, the commission only had two legislative proposals: first to penalize unlawful disclosures of classified information by persons outside as well as within the government (in the past, only disclosures by government employees had been punishable); second, to make admissible in court evidence of subversion that federal agencies had obtained by wiretapping.”⁴⁷ The commission did not specifically address classification, other than to express concern that the classification system could be used to hide mistakes and abuses.

THE 1960s – CONCERNS CONTINUE

As noted previously, Congress passed the original version of the Freedom of Information Act in 1967. The Act was intended to make available to the general public

⁴⁶ Moynihan, 172-173.

⁴⁷ Moynihan, 166.

information held by government agencies. All federal agencies, including agencies such as the Central Intelligence Agency (CIA), were subject to the provisions of the act. However, the CIA obtained exemption from the Act while others, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) simply ignored the provisions of the Act. These agencies continued with a “business as usual” attitude, that the information in their files could not be released to the public.

The Defense Science Board established its Task Force on Secrecy in late 1969 to evaluate the relevance of classifying information. Its focus was on all aspects of the scientific process: research, development, testing, and evaluation, as well as procurement and deployment of complete systems, such as radars, radio sets, etc. Under the chairmanship of Dr. Frederick Seitz, the Task Force submitted its final report to the Director of Defense Research and Engineering on 6 July 1970. Among the Task Force’s findings was a recommendation to limit the amount of time information was to remain classified. While not denying that some information merited safeguarding, they pointed out that strides were made in several fields once the veil of secrecy was lifted. Advances in microwave electronics, computer technology, and research and development on civilian uses for nuclear reactors were cited as being accelerated once classified information was made public.⁴⁸ The Task Force did not dispute classification of intelligence reports, but noted that reporting was part of the same, larger process and merited review.

⁴⁸ Department of Defense, Defense Science Board Task Force on Secrecy, “Defense Science Board Task Force on Secrecy” (6 July 1970), URL: <http://www.fas.org/sgp/othergov/dsbrep.html>, accessed 31 December 1998.

THE 1970s – TIME OF MAJOR CHANGES

During the late 1960s and early 1970s, accusations were made that the United States Government had been spying on its citizens. Operations MINARET and SHAMROCK were revealed as having been established to conduct illegal wiretaps and surveillance of United States citizens. Following the outrage expressed in the press and Congress, both the Senate and House of Representatives established investigative committees to scrutinize the activities of the intelligence agencies. The Church committee in the Senate and the Pike committee in the House conducted sweeping investigations into the use/abuse of authorities granted to the various law-enforcement and intelligence agencies within the United States Government. The outcome of this activity included amending the Freedom of Information Act in 1974 to strengthen it, and passing the Privacy Act, which gave individual citizens the right to obtain records about themselves from the government. Finally, the Senate established the Senate Select Committee on Intelligence in 1974, and the House established the House Permanent Select Committee on Intelligence in 1975 to oversee and monitor all future intelligence activities. Implicit in such an arrangement was the monitoring, questioning, challenging, and validation of classification levels, needs, and reasons. It should be noted that the Congress had the power of oversight before this but chose not to exercise that option. As a result, Congress shares in the blame for the failure of the classification and the accountability systems up to this point.

The Nixon administration established the Interagency Classification Review Committee (ICRC) in May 1972 to monitor implementation of Executive Order 11652, which went into effect on 1 June 1972. Executive Order 11652 replaced the Eisenhower

Executive Order and made some major changes. Individuals were held more accountable and the classification authority now had to be cited on documents. A review of individuals who had the authority to classify information was undertaken to reduce that number, and efforts to review and declassify information over 30 years old began.

The ICRC, under the leadership of Ambassador John S.D. Eisenhower, began its work in May 1972, providing its first report the following May. The committee's findings are examined in the following chapter. Briefly, the committee reported a major reduction in the number of government officials with the originator classification authority, dropping from 59,316 to 21,277. Of those, 7,136 had been authorized to classify material as "Top Secret." That number was reduced to 1,707.⁴⁹ The committee also examined declassification efforts and indexing of classified data.

Although President Nixon, a Republican, established the committee, its work continued under President Carter, a Democrat. This was due in large part to continued resistance within the intelligence community to change. For example:

At the time [Admiral Stansfield] Turner was DCI [Director of Central Intelligence], about fifty codewords were in use in the intelligence community. Turner believed that this system was complicated, cumbersome, and inefficient. He thought that a system consisting of fifty different compartments was both difficult to enforce and inefficient. Turner proposed consolidating the fifty-odd codewords into a system of just five. He was opposed by program managers at NSA and other agencies who, naturally, were inclined to defend their organizational turf and feared that intelligence sources for which they were responsible would be compromised. These program managers stalled in implementing Turner's directive, so that by 1981 Turner had left and the agencies continued to control their own codewords.⁵⁰

⁴⁹ Interagency Classification Review Committee, *Progress Report, Implementation of Executive Order 11652 on Classification, Declassification and Safeguarding National Security Information* (Washington DC: GPO, March 31, 1973), 3. Cited hereafter as the Interagency Classification Review Committee.

⁵⁰ Bruce D. Berkowitz and Allan E. Goodman, eds. *Strategic Intelligence for American National Security* (Princeton, NJ: Princeton University Press, 1989), 113.

The committee represented a bipartisan effort, since both political parties supported its work. As a result, the committee was replaced in 1978 with a permanent body, the Information Security Oversight Office (ISOO). The ISOO continues its work today, reporting to the President every August. Its work forms the core of current efforts to assess the cost of classification.

THE 1980s – HALTING STEPS

The 1980s saw the Republican Party return to power. This return was accompanied by a conservative approach to classification issues. The Reagan presidency issued Executive Order 12356, which, most importantly, changed classification limits from the 25 years imposed by the Carter administration to an indefinite length of time. The argument made was that, in the aftermath of the Church and Pike Committee investigations and the Carter administration's efforts to balance the need for secrecy against the public's need to know, too much sensitive information was being made public. Thus, the Reagan administration attempted to clamp down on the amount of sensitive information being released.

Secretary of Defense Caspar Weinberger established the Department of Defense Security Review Commission on June 25, 1985, in the aftermath of the Walker spy-ring arrests. The Commission reviewed the policies, programs, and procedures then in use by the Department of Defense. Meeting from June through November 1985, the Commission conducted 17 separate formal sessions and numerous informal sessions, interviewing witnesses from all branches of federal government and private industry.

The Commission focused on protecting classified information, but did not address either special compartmented classified information or sensitive but unclassified information. Both areas were considered to be outside the scope of the Commission's charter.⁵¹

The Commission noted that in 1984 the Department of Defense had classified approximately 16 million documents. Although the Commission did not know how many classified documents were being maintained by the Department of Defense at that time, the Commission believed that an estimate of 100 million documents would be realistic.⁵² The Commission estimated that the Department of Defense was responsible for approximately 90 percent of the clearances held by personnel in the Executive Branch, or approximately 2.6 million clearances. Industry accounted for another 1.2 million clearances.⁵³ The Commission reported that, based on the estimated number of classified documents in 1984, "...too much information appears to be classified and at higher levels than is warranted."⁵⁴ As a point of interest, the Commission reported that personnel with original classification authority within the Department of Defense had decreased to 2,296 individuals, including 504 with the authority to classify documents at the top secret level and 1,423 with the authority to classify documents at the secret level. Those figures were down from a total of 8,973 in 1972, including 576 having top secret

⁵¹ Department of Defense Security Review Commission, *Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices* (Washington DC: GPO, 19 November 1985), 2-3. Cited hereafter as Department of Defense Security Review Commission.

⁵² Department of Defense Security Review Commission, 18-19.

⁵³ Department of Defense Security Review Commission, 19.

⁵⁴ Department of Defense Security Review Commission, 49.

authority and 3,647 having secret authority.⁵⁵ Clearly, some forward strides had taken place during the 1970s and early 1980s to get a handle on classification issues.

The Commission also recommended that the open-ended classification practice then in use be stopped. It recommended prohibiting "... the retention of classified documents which are not 'permanently valuable records of the government' more than five years from the date of origin, unless specifically authorized in accordance with record disposition schedules established by the component head."⁵⁶ In other words, the Commission recommended that a validation test be applied. While it did not admit it openly, the implied message was that over-protection of information was viewed as a problem and needed to be addressed. Aside from recommending a full audit of then current holdings, the Commission also recommended annual "clean-out" days for reviewing classified information,⁵⁷ better oversight through improved security awareness and training programs,⁵⁸ and increased manning in the oversight office.⁵⁹ The Commission recommended that better coordination within the Office of the Secretary of Defense (OSD) among the offices that share oversight responsibilities, such as the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASDC3I) and the Deputy Under Secretary of Defense for Policy (DUSD(P)) be instituted,⁶⁰ to avoid duplication and improve oversight.

⁵⁵ Interagency Classification Review Committee, appendix A, 1.

⁵⁶ Department of Defense Security Review Commission, 57.

⁵⁷ Department of Defense Security Review Commission, 58.

⁵⁸ Department of Defense Security Review Commission, 89.

⁵⁹ Department of Defense Security Review Commission, 91.

⁶⁰ Department of Defense Security Review Commission, 82.

THE 1990s – STUDIES AND COMMISSIONS CONTINUE

The Joint Security Commission studied security in 1993 and 1994. The Commission issued its report 28 February 1994 to both the Secretary of Defense and the Director of Central Intelligence. The Commission undertook a full review of the security system – from physical security and background investigations, to levels of classification used in the United States government. The Commission addressed both the offensive side of security as well as the defensive side, that is, how the United States protects information obtained from foreign sources and how the U.S. government protects its information from foreign exploitation. Of special interest was the fact that the Commission recognized that risk could not be avoided at all times. Therefore, it focused on risk management. It identified a five-step process in executing risk management: 1) asset valuation and judgment about consequence of loss; 2) identification and characterization of the threats to specific assets; 3) identification and characterization of the vulnerability of specific assets; 4) identification of countermeasures, costs, and tradeoffs; and, 5) risk assessment.⁶¹

The Commission turned its attention to the current classification system, noting that although the classification system deals “...with only a small slice of the government information that requires protection ... it drives the government’s security apparatus and

⁶¹ Joint Security Commission, *Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence* (Washington DC: GPO, February 28, 1994), 5. Cited hereafter as Joint Security Commission.

most of its costs.”⁶² Despite the studies and recommendations made in the 1950s, 1960s, 1970s, and 1980s, the Commission found that the classification system had grown out of control, with security rules that had become increasingly complex and inconsistent, especially since security officials at different agencies imposed different rules on their specific programs. In the Commission’s words:

[T]he current classification system starts with three levels of classification (Confidential, Secret, and Top Secret), often referred to collectively as collateral. Layered on top of these three levels are at least nine additional protection categories. These include Department of Defense Special Access Programs (DoD SAPs), Department of Energy Special Access Programs, Director of Central Intelligence Sensitive Compartmented Information Programs (DCI SCI), and other material controlled by special access or “bigot” lists such as the war plans of the Joint Chiefs of Staff and the operational files and source information of the CIA Operations Directorate. Further complicating the system are restrictive markings and dissemination controls such as ORCON (dissemination and extraction of information controlled by originator), NOFORN (not releasable to foreign nationals), and “Eyes Only.”⁶³

Further complicating the situation, the Commission reported that:

Within the Intelligence Community, the term Sensitive Compartmented Information (SCI) refers to data about sophisticated technical collection systems, information collected by those systems, and information concerning or derived from particularly sensitive methods or analytical processes. Specific SCI control systems serve as umbrellas for protecting a type of collection effort or type of information. Within each SCI system are compartments and within them, subcompartments, all designed to formally segregate data and restrict access to it to those with a need-to-know, as determined by a central authority for each system. There are over 300 SCI compartments (recently reduced from over 800) grouped in a dozen or so control channels. Special activities have their own non-SCI control channels. Rules relating to SCI programs are found in DCI Directives (DCIDs), but implementation is uneven and minimum standards are often exceeded.⁶⁴

⁶² Joint Security Commission, 7.

⁶³ Joint Security Commission, 7-8.

⁶⁴ Joint Security Commission, 9.

The Commission concluded that the bureaucracy providing security was both costly and complicated. It recommended streamlining the entire system, beginning with the levels of classification. It proposed a one-level classification system, with information being either classified or not. It also proposed a "... single legal definition of classified information and no need to pretend that we can precisely measure the amount of damage to national security that would be caused by unauthorized disclosure."⁶⁵ Simplification of the classification system would lead to a simplification of the security system.

Three years later the Commission on Protecting and Reducing Government Secrecy issued *Report of the Commission on Protecting and Reducing Government Secrecy 1997*. Chaired by Senator Daniel Patrick Moynihan and Congressman Larry Combest, the Commission reported its finding to President Clinton on 3 March 1997. It conducted one of the most thorough and comprehensive studies of government secrecy ever done.

The Commission noted "...five major categories of information are protected through some form of government secrecy: (1) national defense information, encompassing military operations and weapons technology; (2) foreign relations information including that concerning diplomatic activities; (3) information developed in the context of various law enforcement investigations; (4) information relevant to the maintenance of a commercial advantage (typically proprietary in nature); and (5) information pertaining to personal privacy."⁶⁶

⁶⁵ Joint Security Commission, 10.

⁶⁶ Commission on Protecting and Reducing Government Secrecy, *Report of the Commission on Protecting and Reducing Government Secrecy 1997* (Washington DC: GPO, March 1997), 5. Cited hereafter as Commission on Protecting and Reducing Government Secrecy.

The Commission viewed “government secrecy ... as a form of government regulation. With the exception of the procedures for classifying ‘nuclear-related information’ under the Atomic Energy Act and protecting intelligence ‘sources and methods’ under the National Security Act, the mechanics for protecting national security information have evolved through a series of executive orders. Over the past half century, the Congress has played only a limited role in any consideration of how the system should function, limiting itself to occasional oversight hearings. The Executive Branch has assumed the authority both for structuring the classification system and for deciding the grounds upon which secrets should be created and maintained. Thus, what commonly is referred to as ‘government secrecy’ more properly could be termed ‘administrative secrecy’ or ‘secrecy by regulation.’”⁶⁷

The Commission noted that risk management had become a management practice among the various agencies. In addition, the number of original classification authorities had continued to diminish, according to ISOO statistics. “The number of special access programs and compartments designed to provide additional protection beyond that of the Confidential, Secret, and Top Secret levels has been reduced. Progress has been made in moving large quantities of information out of the remaining compartments and programs and into the three classification levels, where it is more easily used by a broader range of ‘customers.’”⁶⁸ All the same, the Commission noted that “...(t)here are approximately 150 DoD (Department of Defense)-approved SAPs (Special Access Program) (the exact number is classified and others have been created but not yet formally approved), down

⁶⁷ Commission on Protecting and Reducing Government Secrecy, 5.

⁶⁸ Commission on Protecting and Reducing Government Secrecy, 19.

from 200 in the late 1980s, and approximately 300 SCI (Sensitive Compartmented Information) compartments, compared with an estimated 800 in the late 1980s.⁶⁹

According to the Commission:

Executive Order 12958, like prior orders, lays out the rules governing the identification and protection of information, the unauthorized disclosure of which could cause “damage to the national security. The now-common practice of specifying categories of information eligible for classification began in 1978 when President Carter’s Executive Order 12065 set out seven such categories, an approach seen at the time as a possible way to reduce initial classification actions. Examination of the Carter Order and subsequent orders, however, reveals only the slightest difference in the *kinds* of information eligible for classification under each. Two categories (confidential sources and cryptology) under President Reagan’s Executive Order 12356 were combined with other categories under Executive Order 12958. The so-called “catch-all” category that allowed agency heads to classify “other categories” of information was rarely invoked, and was deleted under Executive Order 12958.⁷⁰

The Commission also noted that the National Security Act of 1947 tasked the Director of Central Intelligence (DCI) with protecting “intelligence sources and methods from unauthorized disclosure” and that executive orders issued since 1978 specifically authorized classification of sources and methods of information. An extensive classification system was still four years away when the National Security Act of 1947 charged the DCI with protecting methods and sources, so classification became an early tool for the DCI to meet this statutory obligation.⁷¹

In contrast, the Atomic Energy Act authorized “... an entirely separate system for protecting information from that established by executive order. This distinct system

⁶⁹ Commission on Protecting and Reducing Government Secrecy, 27.

⁷⁰ Commission on Protecting and Reducing Government Secrecy, 21-22.

⁷¹ Commission on Protecting and Reducing Government Secrecy, 23.

arose from the desire to establish a special regime for protecting highly sensitive nuclear-related information, coupled with the absence of any formal classification system among civilian agencies immediately after World War II.”⁷² This system remains the only clearly legislated classification system in the United States government.

The Commission noted that “the difficulty of discerning who truly needs access to classified information has contributed to the rise of a host of methods for limiting such access. A variety of control markings and handling caveats restricts the dissemination of information and has added extra layers to the classification system.”⁷³ The Commission reported that special access programs have, to an extent, contributed to the problem. These programs are compartments at the top secret level, that is, they are layers at the top secret classification level.

Building on the work performed by the Joint Security Commission, the Commission on Protecting and Reducing Government Secrecy addressed the special access programs both in the Department of Defense and the intelligence community. The Commission noted that the Department of Defense created a Special Access Program Oversight Committee (SAPOC) in 1994 to “standardize and formalize the approval, termination, revalidation and restructuring procedures for DoD special access programs.”⁷⁴ The programs are reviewed annually, in accordance with Executive Order 12958. Likewise, “within the Intelligence Community, the Controlled Access Program Oversight Committee (CAPOC) performs much the same function as the SAPOC,

⁷² Commission on Protecting and Reducing Government Secrecy, 23.

⁷³ Commission on Protecting and Reducing Government Secrecy, 25.

⁷⁴ Commission on Protecting and Reducing Government Secrecy, 27.

including annual review of all such programs as required by Executive Order 19258 and a report to the Congress. The CAPOC includes within its review the SCI control system compartments and special access programs funded by the National Foreign Intelligence Program.”⁷⁵

In response to its questionnaire, the Commission found at least 52 different protective markings being used on unclassified information, approximately 40 of which are used by departments or agencies that also classify information. Included among these are widely-used markings such as “Sensitive But Unclassified,” “Limited Official Use,” “Official Use Only,” and “For Official Use Only.”⁷⁶ The Commission expressed its concern that “...the very lack of consistency from one agency to another contributes to confusion about why this information is to be protected and how it is to be handled. These designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information.”⁷⁷

The Commission went on record noting that classification and declassification policy and oversight were not strictly security issues but needed to be viewed as “... information management issues which require personnel with subject matter and records management expertise.”⁷⁸ This distinction is crucial because, as Senator Moynihan later noted in his book, *Secrecy*, “... after the U.S. Army had adopted the three-level classification model used by the British – For Official Use Only, Confidential, and Secret (later Confidential, Secret, and Top Secret) – just what any of the various

⁷⁵ Commission on Protecting and Reducing Government Secrecy, 27.

⁷⁶ Commission on Protecting and Reducing Government Secrecy, 28-29.

⁷⁷ Commission on Protecting and Reducing Government Secrecy, 29.

⁷⁸ Commission on Protecting and Reducing Government Secrecy, 44.

terms meant was never defined.”⁷⁹ Because the terms have yet to be defined, classifying information, and at what level, remains a black art. In addition, determining when to declassify information is dependent on when and at what level the information was originally classified.

The Commission stated:

To improve existing practices, senior officials across all the agencies that classify must exert greater leadership and make it clear to subordinates that reducing secrecy, consistent with national security concerns, is a priority. Policies that either implicitly or explicitly encourage classification without much thought to the consequences of that decision must give way to those that encourage a more balanced consideration of the need for secrecy. Those who classify must be instructed and then evaluated on how they approach their classification responsibilities. Classifiers must be aware that classification means that resources will be spent throughout the information’s life cycle to protect, distribute, and limit access to information that would be unnecessary if the information were not classified. The tools designed to assist those classifiers, including classification guides, must be readily available and reflect current national security realities. Underlying all these reforms is the need for a more stable and consistent classification regime, which over fifty years of Executive Branch regulation has been unable to provide.⁸⁰

In his final four years in office, Senator Moynihan twice attempted to introduce legislation to make classification a statute-based activity. His bill was originally introduced as S.712 during the second session of the 105th Congress and titled *Government Secrecy Reform Act of 1998* but did not pass out of the Senate. It was reintroduced in 1999 as S.99. The bill, if it had been enacted, would have designated the President as the authority for all classification issues. It would have provided a consistent classification system for all branches of government. Additionally, it would have acted

⁷⁹ Moynihan, 217.

⁸⁰ Commission on Protecting and Reducing Government Secrecy, 45-46.

as an enabler to control what is classified and who is bound by the rules, providing an authority to define the levels of classification and their appropriate application.

YEAR	COMMITTEE, COMMISSION OR TASK FORCE NAME
1955	The Moss Subcommittee – Special Government Information Subcommittee
1956	Committee on Classified Information
1957	Commission on Government Security
1969	The Defense Science Board Task Force on Secrecy
1971	The Interagency Classification Review Committee
1974	The Church Committee
1974	The Pike Committee
1978	The Information Security Oversight Office
1985	The Department of Defense Security Review Commission
1993	The Joint Security Commission
1997	Commission on Protecting and Reducing Government Secrecy

Table 2 – Review Committees

Source: Author created

CHAPTER 3

GETTING A HANDLE ON CLASSIFICATION

THE ICRC – TRYING TO PUT THE GENIE IN THE BOTTLE

The Nixon Administration established the Interagency Classification Review Committee (ICRC) in June 1972 under the auspices of Executive Order 11652. The Committee was charged with meeting at least once a month to develop methods to:

... (a) prevent overclassification, (b) ensure prompt declassification in accord with the provisions with the Order (EO 11652), (c) facilitate access to declassified material, and (d) eliminate unauthorized disclosure of classified material.⁸¹

In the introduction to its first report, however, the ICRC noted that during the first six months it had:

emphasized the development of sound procedures for dealing with security classification problems and the establishment of a viable reporting system for evaluating departmental classification programs. ... Specifically, the ICRC ha(d) focused its attention upon reduction in Government officials with classification authority, review and approval of departmental implementing regulations, establishment of a quarterly reporting system, implementation the data index requirement, and education of Federal employees on changes adopted by the new Order.⁸²

Even though it was not part of the mandate, this action translates into cost accounting. By examining the number of classifiers throughout the government and the amount of classified material reported each year, one can gain a better understanding of past costs.

⁸¹ Interagency Classification Review Committee, 1.

⁸² Interagency Classification Review Committee, i

Initially the ICRC focused its attention on the number of personnel within the federal government authorized to classify information without the need to obtain higher authority approval. Table 3 is derived from ICRC reporting from 1971 through 1977 and lists the total number of personnel with such authority. The table presents this data by classification levels. Classification authority builds in a progressive fashion. Personnel authorized to classify material at the confidential level can not classify information above that level. Those authorized to classify at the secret level are also authorized to classify information at the confidential level, but not at the top secret level. The authority to classify information at the top secret level includes the authority to classify information at the secret and confidential classification levels.

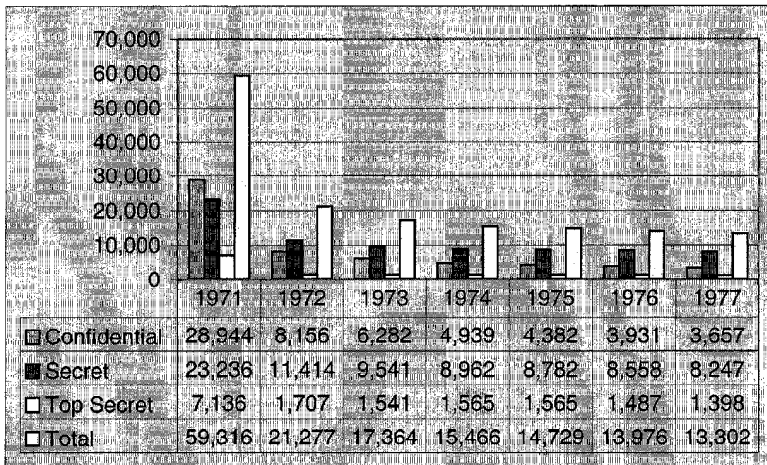


Table 3 – Original Classification Authorities from 1971 to 1977

Source: ICRC Reports 1971 – 1977

As the chart indicates, the number of authorized original classification authorities (OCA) throughout the government was extremely high. Since various individuals can and often do interpret information in different ways, it is likely that the same information could possibly have different levels of classification. Reducing the number of OCAs marked a major first step towards understanding the cost of classification actions.

The ICRC was also involved in determining the total number of classification actions in each year, reporting data two years after it took up its mandate. The focus was on original classification actions, i.e., new and unique material that was classified for the first time. The ICRC did not address the issue of derivative classification, information already deemed sensitive enough to merit classification with personnel using existing classification guidance to classify that information. Therefore, the number of derivatively classified documents created by government workers until 1979 is unknown. Table 4 contains totals for original classification decisions and is derived from ICRC reports from 1973 through 1977. As mentioned above, the ICRC did not report on decisions during the first two years.

By the time the first classification decisions were reported, the number of government-wide OCAs had been reduced by more than two-thirds. In the successive years the number reduced again by approximately one-third, going from 17,364 in 1973 to 13,302 in 1977. Interestingly, the total number of original classification decisions actually increased by approximately 400,000 decisions, going from 4,086,319 in 1973 to 4,487,333 in 1977. It is possible that methodologies for information collection and reporting could have changed over time; the reports from this period do not address this question. The ICRC reported in its initial report that it would gather statistics on a

quarterly basis but did not elaborate on what method(s) would be used so it is not possible to know if data was gathered daily, once a week, once a month or once a quarter. It is also unknown what time limits were imposed if the data collection was not done daily, that is, if the data was collected for a one, two, three, or four day period each week, or if the data was gathered once a week each month, etc. Each agency could have imposed its own method of data collection, at variance with any standards that may have been prescribed.

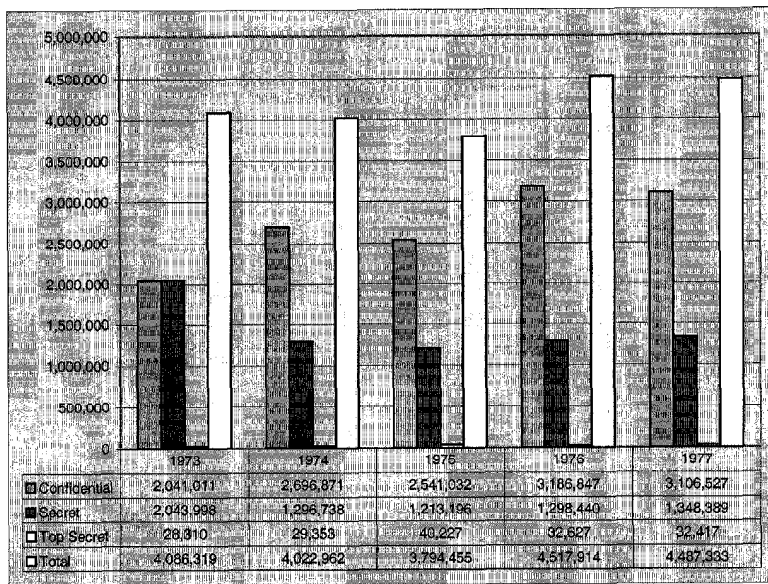


Table 4 – Original Classification Decisions from 1973 to 1977

Source: ICRC Reports 1973-1977

The ICRC did not examine the cost of classifying information; this task was added subsequently by the ISOO. While the ICRC mentioned the misuse of classification

as a possible way to bury mistakes, it did not produce any statistics on this issue. The ICRC conducted its business during the era of the Pike and Church Commissions and investigations of the intelligence community, a time of turmoil and distrust of Congress and any other investigative body by the intelligence community. Thus, it is impossible to determine whether no statistics existed based on non-pursuit of the issue or based on IC resistance.

Even though the ICRC had a limited mandate and worked with some significant obstacles in its path, the committee made the first real attempt to get a handle on what was going on within the government regarding classification issues. Its findings led to a tightening of the guidelines concerning who can be an original classification authority. It also published, for public scrutiny, the number of original classification decisions made each year. The reports were not categorized by specific agencies; e.g., all military and civilian intelligence agencies within the Department of Defense were grouped together under the Department of Defense. Nonetheless, for the first time, it provided an estimate of the amount of classification within the government. The committee ended its work in 1977, submitting its final report in 1978. The ICRC recommended that its work be continued with an expanded mandate.

THE ISOO – CONTINUING THE WORK

The Information Security Oversight Office (ISOO) was established in 1978 and continued the work begun by the ICRC. An under-funded and understaffed organization, the average annual budget in the 1980s was \$500,000.00 to \$700,000.00. The ISOO did

not always get the full cooperation of the various government agencies it was formed to monitor.

The ISOO reports its findings once a year, following the fiscal year cycle of 1 October - 30 September of the following calendar year. It requires that reports be submitted annually. In some cases, such as with the Department of Defense and the Central Intelligence Agency, the ISOO has occasionally approved the sampling methods used to gather data for the annual report.⁸³

The ISOO issued its first report in 1980 on oversight activity conducted in 1979 (no data were collected in 1978 during the transition period from the ICRC). The ISOO expanded the range of its examinations, including information on derivative classification actions, as well as continuing to monitor the total number of original classification authorities and original classification activity. Significantly, the ISOO began looking more closely at mandatory declassification activities and erroneous classifications, including items either under or over classified.

Table 5 is a list of the original classification authorities (OCA) in the United States government between the years of 1979 and 1989. The number of OCAs in the government was cut in half between 1977 and 1979, decreasing from 13,302 to 6,927. That number remained relatively steady throughout most of the decade, reduced by only approximately another 500 or so by the end of the decade.

The ISOO began keeping records of derivative classification during this time. It also attempted to count the number of derivative authorities during 1979 and reported those figures, but stopped reporting that information afterwards. Although no reason was

⁸³ Information Security Oversight Office, *Annual Report to the President FY 1985* (Washington, DC: GPO, 1986), 7

given for ending the practice, it was undoubtedly done because any individual with a security clearance and charged with writing classified documents would be considered a derivative classification authority by definition. Therefore, the number of personnel holding a security clearance should equal the number of derivative classification authorities. Since the government already keeps records on the number of personnel with clearances, no new information is gained by collecting and reporting this information.

Table 6 is provided for background information.

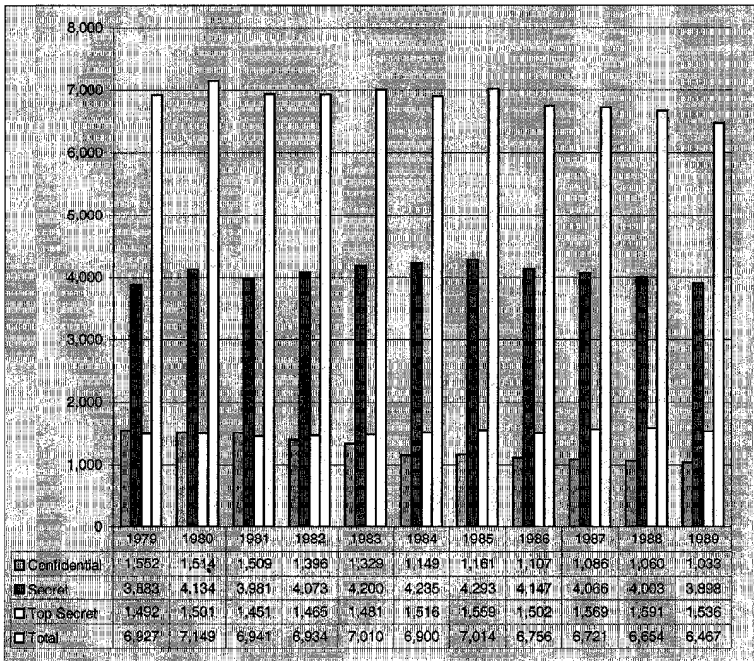


Table 5 – Original Classification Authorities from 1979 to 1989

Source: Reports for 1979 – 1989

Derivative Classifiers Government-wide in 1979	
Confidential	32,945
Secret	97,287
Top Secret	110,693
Total	240,925

Table 6 – Derivative Classifiers Government-wide in 1979

Source: ISOO Report for 1979

The ISOO broke out classification levels for original and derivative classification decisions in 1979 but only reported totals in 1980 and 1981. Tables 7 and 8 show original and derivative classifications made during the 1979 to 1981 timeframe.

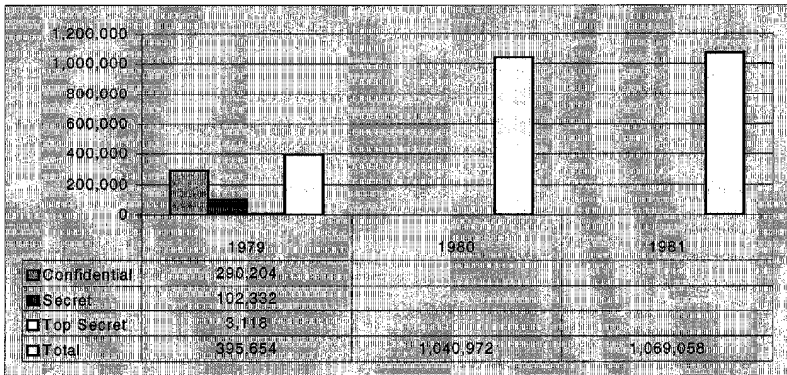


Table 7 – Original Classification Decisions 1979 to 1981

Source: ISOO Reports 1979-1981

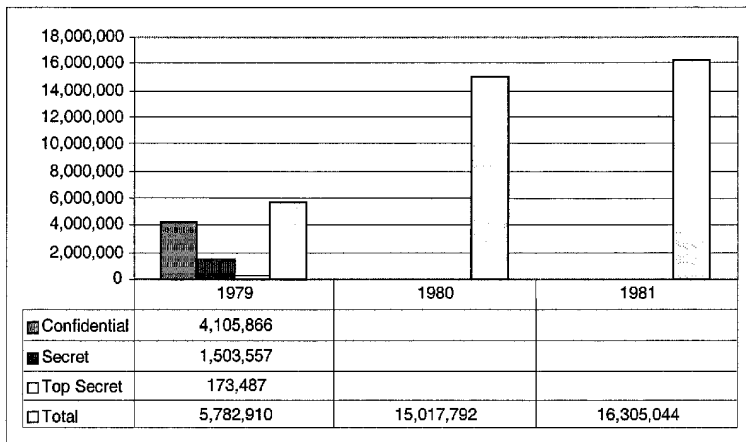


Table 8 – Derivative Classification Decisions 1979 to 1981

Source: ISOO Reports 1979-1981

The figures reported in 1979 were based on a five-month statistical collection, from May through September 1978. The number of original decisions at all levels totaled 395,654; derivative totaled 5,782,910. As a ratio, the number of original decisions to derivative was approximately 1:14 or, viewed another way about seven percent of the decisions made that year were original in nature. Statistically, this does not differ very much from 1980, when the ratio was approximately 1:15 and 1981, when the ratio increased to 1:16. If the five-month total of 6,178,564 is divided by 5 and multiplied by 12, the figure derived for 1978 is 14,828,554. This number is similar to the combined original and derivative decisions in 1980 of 16,058,764 and in 1981 of 17,374,102. Simultaneously, the number of OCAs for these three years varied only slightly from 6,927 in 1979 to 7,149 in 1980 and back down to 6,941 in 1981.

Tables 9 and 10 display the total original and derivative classification decisions made from 1982 through 1989. The number decreased over time, dropping by approximately one-half at all three levels from 1982 to 1989. The number of derivative classification decisions dropped even more dramatically from 16,449,459 in 1982 to 6,294,707 in 1989. However, the number of top secret classification decisions doubled from 493,484 in 1982 to 892,055 in 1989; secret-level classifications remained fairly constant throughout; and confidential classifications dropped from a high of 11,021,137 in 1982 to 1,046,033 in 1989, accounting for the steep decline.

Whether classification guidance was poorly understood and implemented by the workforce or there was simply more data that merited greater protection is a question that can not be answered. While the numbers indicate an overall reduction in the amount of classified materials, the breakdown by levels indicate that more material was classified at the top secret level. Savings that may have been realized from the less stringent safeguarding of confidential material were consumed, instead, by protecting the increased level of top secret material.

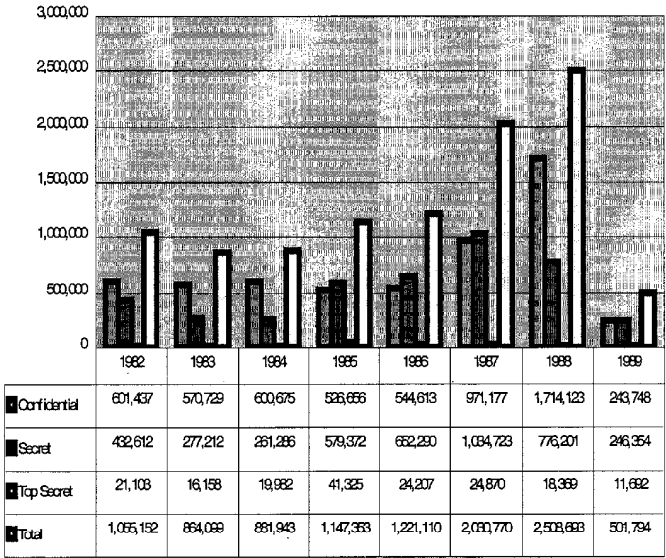


Table 9 – Original Classification Decisions 1982 to 1989

Source: ISOO Reports 1982 to 1989

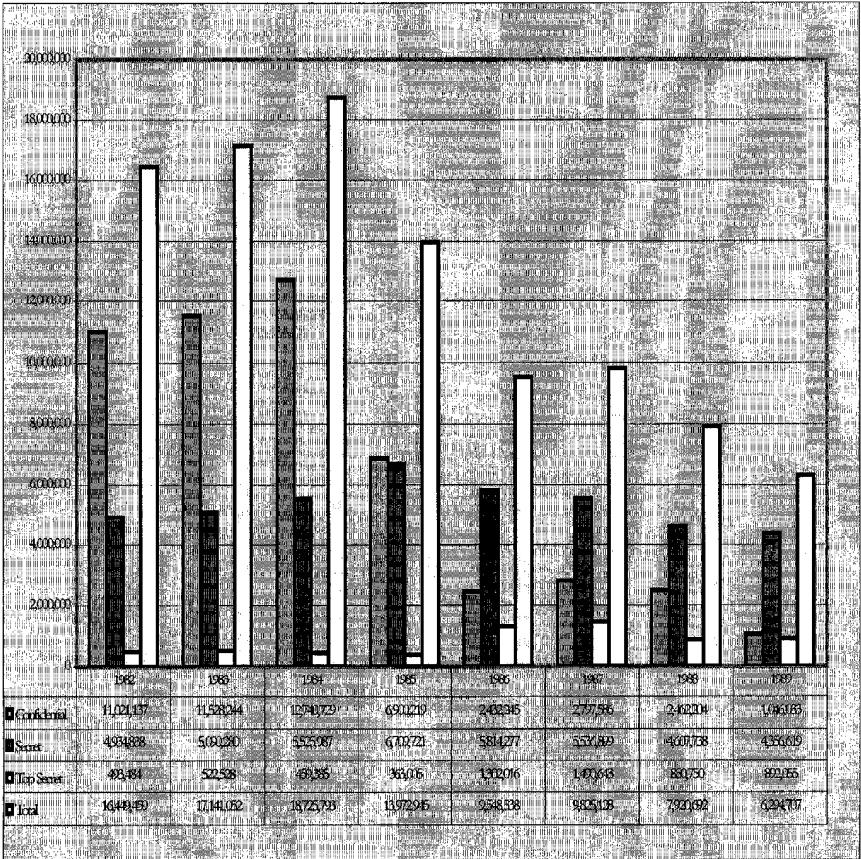


Table 10 – Derivative Classification Decisions 1982 to 1989

Source: ISOO Reports 1982 to 1989

<i>Year</i>	<i>Original Decisions</i>	<i>Derivative Decisions</i>	<i>Ratio</i>
1980	1,040,972	15,017,792	1:15
1981	1,069,058	16,305,044	1:16
1982	1,055,152	16,449,459	1:16
1983	864,099	17,141,052	1:20
1984	881,943	18,725,793	1:21
1985	1,147,353	13,972,945	1:12
1986	1,221,110	9,1548,538	1:8
1987	2,030,770	9,825,128	1:5
1988	2,508,693	7,920,692	1:3
1989	501,794	6,294,707	1:13

Table 11 – Ratio of Original to Derivative Classification Decisions in the 1980s

Source: ISOO Reports from FY 1980 to FY 1989

The figures in Table 11 offer another way of viewing the classification activity of the 1980s. While the aggregate numbers decreased towards the end of the decade, the number of original decisions made from 1986 through 1988 increased significantly. The ratio of original decisions vice derivative went from 12.5 percent in 1986, to 20 percent in 1987 and 33 percent in 1988. The number returned to the average amount of 7.67 percent in 1989. This was a time of major changes in the Soviet Union and Soviet bloc nations, with the Gorbachev regime in the Soviet Union entering its period of openness and may offer a partial explanation of the anomalous figures.

The ISOO continued its work through the 1990s. In addition to accounting for OCAs and determining the number of original and derivative classification decisions made annually, the ISOO gathered figures to attempt to assign a dollar value to the classification process. Prior to 1995 no such attempt had been made.

Table 12 lists the number of OCAs in the government between 1990 and 1999.

As noted, the totals continued to decline, with less than 4,000 individuals in the government having the authority to make original classification decisions at the end of FY 1999.

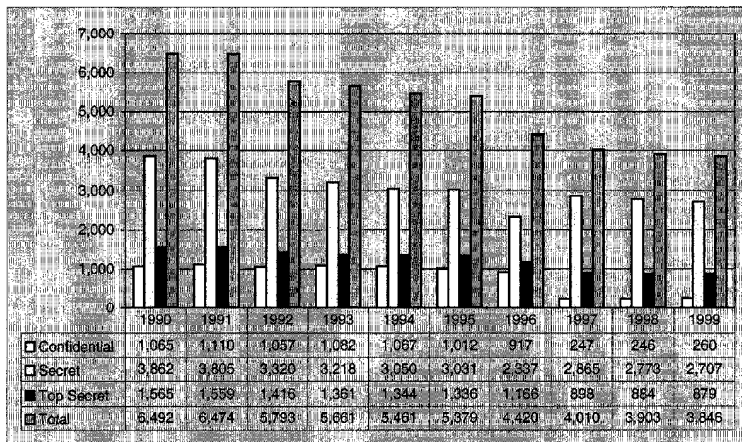


Table 12 – Original Classification Authorities 1990 to 1999

Source: ISOO Reports 1990 to 1999

Tables 13 and 14 compare the original and derivative classification decisions made in the government during the 1990s. By the middle of the decade, the total number of original classification decisions had decreased from just under 500,000 to 167,840 in 1995, a reduction approximately two-thirds. The figure continued to drop to 105,163 in the following year, but then began to climb again. For the decade the number of top secret decisions decreased from 14,344 to 3,601 or more than 75 percent. Secret decisions dropped by 50 percent, declining from 256,329 in 1990 to 125,903 in 1999.

Confidential decisions changed the most, decreasing from 220,302 in 1990 to 40,231 in 1999; an approximate decline of 92 percent for the decade.

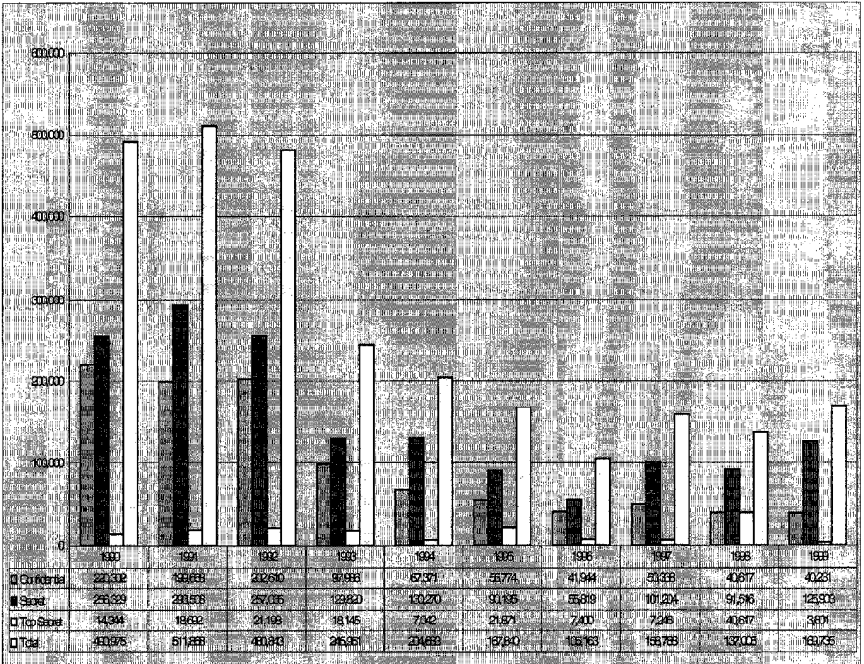


Table 13 – Original Classification Decisions 1990 to 1999

Source: ISOO Reports 1990 to 1999

Table 14 provides ISOO data reported for derivative classification during the 1990s. What is apparent from the numbers is that the business of classification has remained unchanged. The classifiers were busier as the decade progressed. The total number of derivative classification decisions increased from 6,306,745 in 1990 to 7,868,857 in 1999. All three levels of classification experienced increases throughout the

1990s. Although there was a downturn in the mid-1990s, during the same timeframe that the Clinton administration drafted and issued Executive Order 12958 on classification, the numbers started to rise again shortly afterwards.

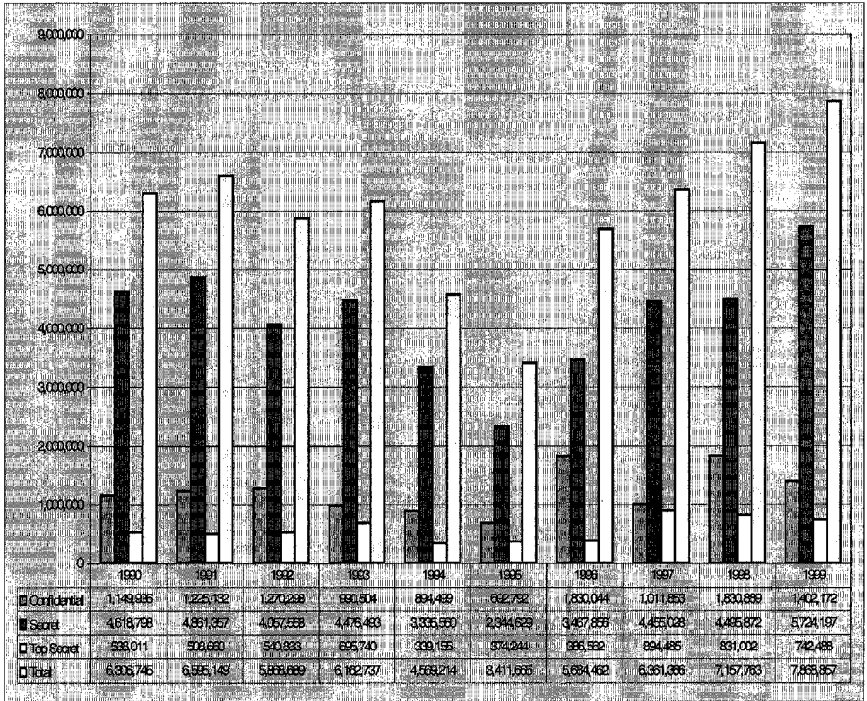


Table 14 – Derivative Classification Decisions 1990-1999

Source: ISOO Reports 1990 to 1999

<i>Year</i>	<i>Original Decisions</i>	<i>Derivative Decisions</i>	<i>Ratio</i>
1990	490,975	6,306,745	1:13
1991	511,868	6,595,149	1:13
1992	480,843	5,868,689	1:12
1993	245,951	6,162,737	1:25
1994	204,683	4,569,214	1:22
1995	167,840	3,411,665	1:20
1996	105,163	5,684,462	1:54
1997	158,788	6,361,366	1:40
1998	137,005	7,157,763	1:52
1999	169,735	7,868,857	1:46

Table 15 – Ratio of Original to Derivative Classification Decisions during the 1990s

Source: ISOO Reports for FY 1990 to FY 1999

The figures in Table 15 indicate that while the number of original decisions has gone down throughout the decade, the number of derivative decisions has gone up. The indication is that the often touted “peace dividend,” a benefit of the demise of the Soviet Union, has been a myth. The savings supposedly derived from the passing of a “bipolar” world of two superpowers have, instead, been spent on the multi-polar situation of today. Even though the Soviet Union and the Warsaw Pact alliance came to an end in the early 1990s, other issues that had been secondary concerns at that time took center-stage. Problems such as international terrorism and the international narcotics trade have become major concerns.

Rogue states, such as Cuba, North Korea, Iran and Iraq continue to be sources of concern for the United States. India has been open in its pursuit of weapons technology and has exploded a nuclear device, prompting an arms race in Southwest Asia with Pakistan and other nations. Political instability has plagued several nations. The native

populations of East Timor and Irian Jaya have challenged Indonesia, portions of that nation that do not identify with the central government in Jakarta. Likewise, the nations of the Balkan region have splintered from Yugoslavia, each determined to exert its independence from the others. Nations in Africa have been torn by tribal strife, which does not recognize the artificial political boundaries that were drawn up by European colonial powers. The same applies to the Middle East. The Palestine Mandate, which created the modern state of Israel at the expense of the Palestinians, is an outgrowth of the Sykes-Picot Treaty of 1916, the divided the Middle East into French and British spheres of influence. The need to address all of these intelligence concerns requires continual monitoring and reporting. The reports, using accepted classification guidelines, create the derivative classification decisions and increased vigilance and reporting that is reflected in these increased numbers.

CHAPTER 4:

PUTTING A PRICE ON THE COST OF CLASSIFICATION

DOLLAR AMOUNTS

Congress mandated placing a dollar amount on the cost of classification as outgrowth of the compromises created by the spying of such people as Aldrich Ames, the Walker family, Ronald Pelton, Jonathan Pollard and others. For many years it was argued that the cost of classification was so closely intertwined with other costs, such as physical and personnel security, that meaningful figures could not be separated out. Nonetheless, Congress prevailed and the mandate to provide dollar cost amounts went forward.

The ISOO began reporting classification costs for both the government and industry in 1995. Table 16 shows the figures reported for the government and industry. According to the ISOO, “Congress first requested security classification cost estimates from the Executive branch in 1994. The Office of Management and Budget reported those cost estimates to Congress while working with agencies to develop better sampling methodology for future years. Congress has continued to seek updated estimates. In addition, ISOO is now tasked through Executive Order 12958 to report these costs to the President.”⁸⁴ The ISOO includes these figures in its annual reports, even though it admits

⁸⁴ Information Security Oversight Office, *1995 Report to the President* (Washington, DC: GPO, 1995), 8.

that the methodology needs refinement. The aim is to establish a baseline that, once enough depth of information is gathered, will provide an adequate indication of costs. The cost each year is in the billions of dollars. The industrial figures are not expanded, the amounts spent on such items as physical security, information security, training, etc, are not provided. The government figures, in contrast, are categorized to present a better idea of costs. Table 17 provides those figures.

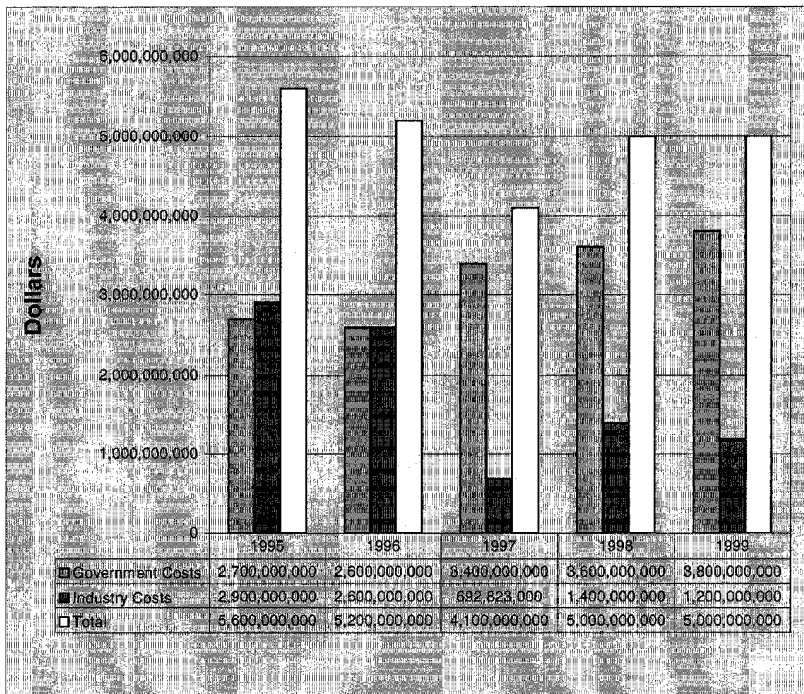


Table 16 – Government and Industry Classification Costs 1995 to 1999

Source: ISOO Reports 1995 to 1999

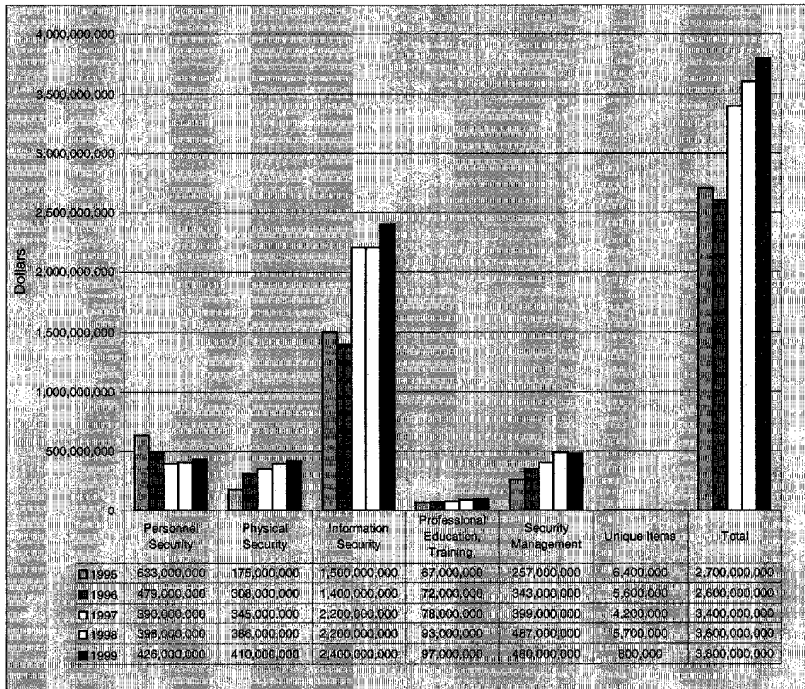


Table 17 – Estimated Government Classification Costs by Category – 1995 to 1999

Source: ISOO Reports 1995 to 1999

Table 18 provides a breakdown for each subcategory. Initially only the costs of classification management and information assurance were addressed. The costs associated with declassification were not listed until 1997. The pie charts in tables 19 through 23 provide the same information in a percentage format.

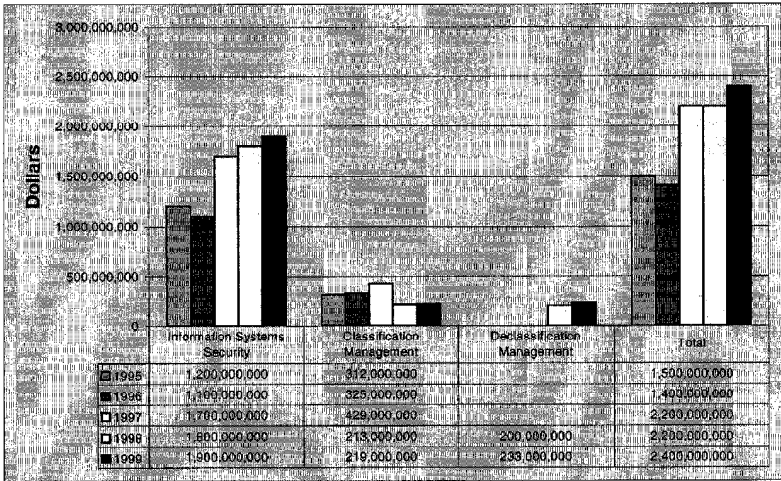


Table 18 – Information Security Cost Estimates 1995 to 1999

Source: ISOO Reports 1995 to 1999

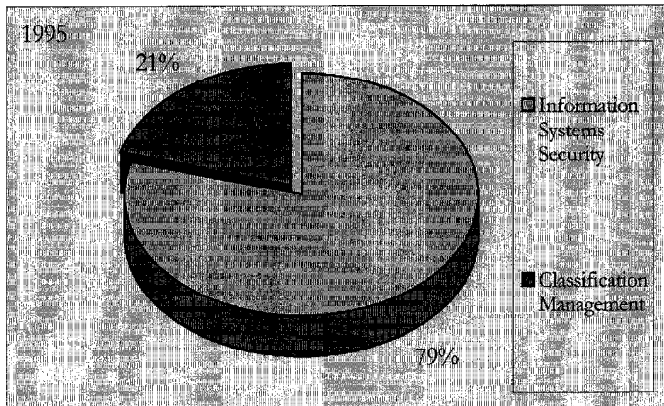


Table 19 – Information Security Costs as Percentages of Dollars Spent – FY 1995

Source: ISOO Annual Report for FY 1995

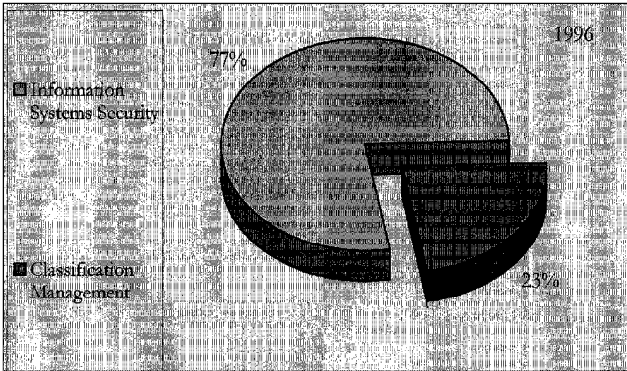


Table 20 – Information Security Costs as Percentages of Dollars Spent - FY 1996

Source: ISOO Annual Report for FY 1996

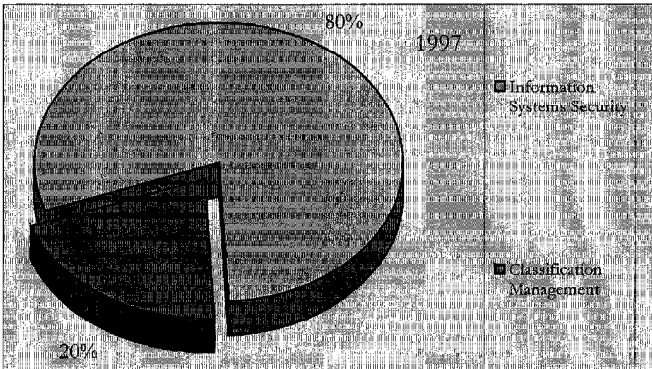


Table 21– Information Security Costs as Percentages of Dollars Spent - FY 1997

Source: ISOO Annual Report for FY 1997

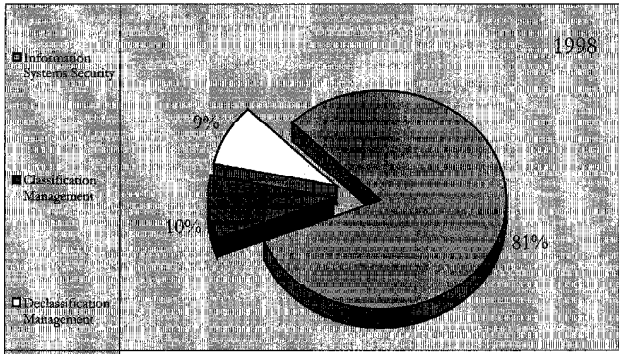


Table 22 – Information Security Costs as Percentages of Dollars Spent - FY 1998

Source: ISOO Report for FY 1998

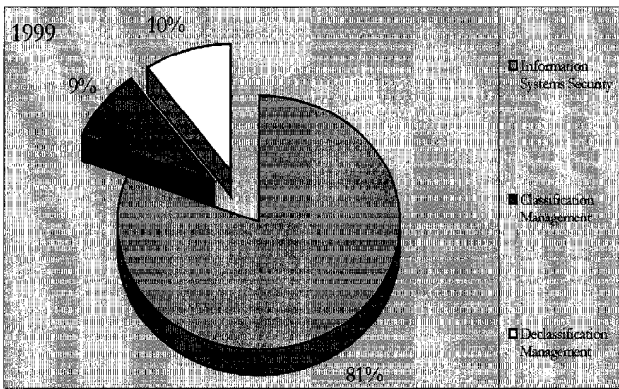


Table 23 – Information Security Costs as Percentages of Dollars Spent - FY 1999

Source: ISOO Annual Report for FY 1999

The figures all point to the fact that, in terms of overall budget, classification management is a small part of the total money spent each year in classification costs. Once classification management is separated from the information security figures, the amount spent each year on classification management is seen to be much less than the amount spent on physical security, personnel security, or security management.

POLYGRAPHS – ANOTHER FORM OF CLASSIFICATION MANAGEMENT

In addition to mandating dollar amounts be reported to it, Congress also directed the Intelligence Community to provide annual reports on its polygraph program. The Department of Defense has complied with this order since 1994. It issues an unclassified report with a classified annex that provides figures for polygraphs administered by the National Security Agency. The Central Intelligence Agency provides a classified report separately for its polygraph efforts. The CIA includes information for National Reconnaissance Office polygraphs. Therefore, while the Department of Defense reports do not account for all of the federal government, they are an indication that a serious effort is being made to manage the human aspects of classification management.

Briefly, the reports include thumbnail studies of what the polygraph process has uncovered. For example, in the report for 2000, an examinee was reported to have mishandled classified information on approximately six occasions, divulging “NATO satellite communications to persons not authorized to receive such information.”⁸⁵ An average of 7,800 polygraphs is conducted each year, according to the annual reports.

⁸⁵ Department of Defense, *Annual Polygraph Report to Congress, Fiscal Year 2000*, URL: <<http://www.fas.org/sppg/othergov/polygraph/dod-2000.html>>, accessed 14 March 2001.

The number of polygraphs reported is very small, when compared with the number of security clearance applications reported as pending. Newspaper reporting during 2000 indicated that anywhere from 500,00 to 900,000 people were waiting for security clearance investigations to be completed. The backlog was blamed on several factors: poorly trained investigators, too few investigators, and too little money allocated for investigation. The risk then becomes that people who should be more closely investigated, or reinvestigated more often, are free to handle classified information. An example of this is Navy Petty Officer Daniel King who was found, during a reinvestigation, to have mailed a classified computer disk to the Russian Embassy.⁸⁶ Efforts are underway to address the investigative problem, but the manning shortfalls continue to this day.

Although debate continues regarding the effectiveness of the polygraph, it should be noted that neither the Federal Bureau of Investigation, which employed Mr. Hanssen, nor the United States State Department, have required polygraphs. The damage inflicted by Mr. Hanssen is currently being investigated. In the case of the State Department, documented instances of mishandling of classified information exist. One of the better known instances deals with the removal of classified documents from then Secretary of State Madeline Albright's desk by an unknown person. The documents have never been found, nor has the culprit ever been apprehended. Instituting routine polygraphs would not only help with better managing personnel and physical security, but indirectly assist with classification management since, in the long run, it is the classified information that

⁸⁶ "900,000 Await Security Clearances," *The Arizona Republic*, 22 April 2000, A6.

is being safeguarded. If there were no classified information to safeguard, there would be no need for the rest of the infrastructure.

CHAPTER 5:

WHY IT DOES NOT ADD UP

THE NEED FOR ACCOUNTING

This concern for accounting has not abated, but instead has intensified with the recent arrest of FBI agent turned Russian spy Robert Hanssen. The Walker family compromised Navy codes while Aldrich Ames provided CIA documents covering terrorism, counterintelligence and other topics. Jonathan Pollard provided intelligence to the Israelis, while Ronald Pelton provided information to the Russians on the United States success against Russian encryption. Their spying activity was wide-ranging, covering a variety of topics at all levels of sensitivity. Although it is well understood that serious damage was done, no one knows just how much material has been compromised because some, such as Ames, took anything they could find, without regard to the contents. As a result, the costs to the United States remain uncalculated.

HOW TO UNDERMINE THE SITUATION

These cost accounting efforts are undermined when a person under investigation is pardoned. President Clinton, prior to leaving office in January 2001, granted a presidential pardon to John Deutch.⁸⁷ Mr. Deutch had been the Director of the Central

⁸⁷ David Abel, "Ex-CIA Chief Deutch Gets Presidential Pardon," *Boston Globe*, 21 January 2001, 25.

Intelligence Agency under President Clinton in the middle 1990s. The computers in his homes in Bethesda, Maryland and Belmont, Massachusetts, as well as his offices in the Old Executive Office Building and CIA Headquarters,⁸⁸ were connected to the Internet. Members of his household had access to them. Despite the unsecured nature of these computers, he kept extremely sensitive, classified information⁸⁹ on them in violation of security guidelines, which he, as the Director of Central Intelligence, was obliged to enforce. Mr. Deutch was subsequently investigated and was found negligent.⁹⁰ He was prepared to admit guilt when the presidential pardon was granted. Thus, the very rules put in place to warrant the safety of classified information were compromised by the men charged with enforcing them.

Because of this, all of the efforts made to account for classification and the associated costs must be called into question. The costs that are not reported but which need to be included are estimates of how much such compromises cost the taxpayer. A legislative approach must be implemented to govern the classification process. Until that is done the process will remain subject to the fiat of executive orders. Clearly defined penalties, free from the intervention of presidential pardons, need to be enumerated. No individual, regardless of rank or position, should be exempted from the governance process. Whether one willfully sold or passed on classified information, or was arrogantly negligent in discharging his or her duty is immaterial, the resulting damage

⁸⁸ Central Intelligence Agency, *Report of Investigation: Improper Handling of Classified Information by John M. Deutch* (1998-0028-IG), URL: <http://www.fas.org/ikrp/cia/product/ig_deutch.html>, accessed 29 May 2001.

⁸⁹ Bill Gertz, "Ex-CIA Chief Compromised Secrets," *The Washington Times*, 12 October 2000, A1.

⁹⁰ Central Intelligence Agency, *Report of Investigation: Improper Handling of Classified Information by John M. Deutch*.

must to be included in the total cost of classification, if not, then complete accounting is not possible.

SOME SUGGESTED SOLUTIONS

A mechanism currently exists that could be used to correct this situation. President Clinton established the Security Policy Board in September 1994 under Presidential Decision Directive 29. The Board was established to develop security standards and practices. This organization was established at the recommendation of the Joint Security Commission⁹¹ and was originally named the Joint Security Executive Committee. The Board membership comes from approximately 35 government agencies and departments. A major criticism is that the Board does not meet often enough to be effective. Another criticism is that the Board tends to work at the level of the least supportive agency, meaning that the Board works on consensus.⁹² The Board needs to be a more proactive force in the oversight arena.

Senator Daniel Patrick Moynihan, a vocal critic of the CIA and the security and classification process in general has said, "Secrecy is a form of regulation."⁹³ He introduced legislation twice in the Senate that would have reformed the classification process. The bill would have empowered the president to guard against "unauthorized disclosure of any information owned by, produced by or for, or under the control of the

⁹¹ Richard Lardner, "Behind Closed Doors," *GovExec.com*, April 1996 URL: <<http://www.govexec.com>>, accessed 27 December 1999.

⁹² Richard Lardner, "Keeping Secrets," *GovExec.com*, March 1998, URL: <<http://www.govexec.com>>, accessed 27 December 1999.

⁹³ Moynihan, 59.

executive branch when there is a demonstrable need to do so in order to protect the national security of the United States.”⁹⁴ The bill goes on to spell out what criteria are deemed necessary to classify and declassify information. While the substance of the bill varies little from the presidential orders on classification, the upshot to the bill’s passage would have been to make the legislation binding on all branches of the federal government. The fact that the bill never passed out of the Senate during either session for consideration by the House of Representatives is indicative of a lack of will on the part of the politicians to clearly address the problem.

This could be explained, at least in part, by the fact that members of Congress, by virtue of their office, are automatically granted security clearances and do not undergo the same clearance examination process that the average intelligence community worker undergoes. So long as classification is conducted by means of Presidential executive orders, neither the Legislative nor Judiciary branches of government are obligated to observe the guidance given.

Therefore, the time has come to reexamine our current system. If the government truly wants to be able to put a dollar cost amount on classification, a number of things will need to change. First, legislation that is binding on all branches of government must be enacted. Second, clear guidance on what is and is not considered sensitive information must be given to the intelligence community. There also needs to be an agreed upon methodology of how to calculate the cost. Workers would have to provide figures regarding how much of their day is spent in producing, disseminating and safeguarding classified information. This could be incorporated into the biweekly

⁹⁴ U.S. Congress, Senate, *Government Secrecy Reform Act of 1998, as amended*, 105th Cong., 2nd sess., 1998. S. 712.

paysheet as an entry that would be used to calculate, based on the person's annual pay, the cost of safeguarding that information. Third, the hidden costs of physical plant, security, perimeter guards, etc., need to be included in the mix. Fourth, contractors must be given the same guidance so that information created apart from government agencies, but on behalf of the government, is accounted for in the same manner. In other words, the figures must be derived in the same manner, otherwise, the figures might well be at great variance and "skewed" with regards to government figures. Finally, there must be a political will among our leadership to make the rules apply equally to everyone. This means that anyone caught compromising national security must expect full punishment for his or her actions. Presidential pardons and plea-bargaining work to undermine the system, since both activities indicate a lack of seriousness on the part of leadership.

Improving the mechanisms currently in place, instituting a more rigorous standard through an Act rather than through a Presidential order, and adhering to an applying the same set of standards to every transgressor, regardless of rank or position, would be the first positive steps towards improving the classification management system. Once this is done, we as a nation would then be closer to obtaining a true idea of how much information classification really costs us.

BIBLIOGRAPHY

- Adams, James. *Sellout: Aldrich Ames and the Corruption of the CIA*. New York: Viking, 1995.
- Abel, David. "Ex-CIA Chief Deutch Gets Presidential Pardon." *Boston Globe*, 21 January 2001, 25
- Ameringer, Charles D. *U.S. Foreign Intelligence*. Lexington, MA: Lexington Books, 1990.
- Andrew, Christopher. "The Growth of the Australian Intelligence Community and the Anglo-American Connection." *Intelligence and National Security* 4, no. 2 (April 1989): 213-256.
- Angevine, Robert G. "Gentlemen Do Read Each Other's Mail: American Intelligence in the Interwar Era." *Intelligence and National Security* 7, no. 2 (1992): 1-29.
- Aspin-Brown Commission. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. Washington DC, GPO, 1996.
- Bamford, James. *The Puzzle Palace: a Report on America's Most Secret Agency*. Boston MA: Houghton Mifflin Company, 1982.
- _____. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: from the Cold War through the Dawn of a New Century*. New York: Doubleday, 2001
- Barnett, Harvey. "Legislation-based National Security Services: Australia." *Intelligence and National Security* 9, no. 2 (April 1994): 287-300.
- Berkowitz, Bruce D. and Allan E. Goodman. *Strategic Intelligence for American National Security*. Princeton NJ: Princeton University Press, 1989.
- Blais, J. J. "The Political Accountability of Intelligence Agencies – Canada." *Intelligence and National Security* 4, no. 1 (January 1989): 108-118.
- Bozeman, Adda B. *Strategic Intelligence and Statecraft*. NY: Brassey's Inc., 1992.
- Breckinridge, Scott D. *The CIA and the U.S. Intelligence System*. Boulder CO: Westview Press, 1986.

British and American Approaches to Intelligence. Ed. K.G. Robertson. NY: St. Martin's Press, 1987.

Carver, George A., Jr. "Intelligence in the Age of Glasnost." *Foreign Affairs* 69, no. 3 (Summer 1990): 147-166.

Central Intelligence Agency. *Report of Investigation: Improper Handling of Classified Information by John M. Deutch* (1998-0028-IG). URL: <http://www.fas.org/ikrp/cia/product/jg_deutch.html>. Accessed 29 May 2001.

Classified Information Procedures Act. Public Law 96-456, 96th Congress. 15 October 1980.

Codevilla, Angelo. *Informing Statecraft: Intelligence for a New Century*. New York: The Free Press, 1992.

Commission on Protecting and Reducing Government Secrecy. *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy*. Washington, DC, GPO, 1997 Senate Document 105-2.

Comparing Foreign Intelligence - The US, the USSR, the U.K. and the Third World. Ed. Roy Godson. McLean VA: Pergamon-Brassey's International Defense Publishers, Inc., 1987.

Demac, Donna A. *Liberty Denied: The Current Rise of Censorship in America*. 1st rev. ed. New Brunswick, NJ: Rutgers University Press, 1990.

Defense Science Board. *Report of the Defense Science Board: Task Force on Secrecy*. 6 July 1970. URL: <<http://www.fas.org/sgp/othergov/dsbrep.html>>. Accessed 31 December 1998.

Department of Defense. *Annual Polygraph Report to Congress, Fiscal Year 1997*. URL: <<http://fas.org/sgp/othergov/polygraph/dod-1997.html>>. Accessed 14 March 2001.

_____. *Annual Polygraph Report to Congress, Fiscal Year 1998*. URL: <<http://fas.org/sgp/othergov/polygraph/dod-1998.html>>. Accessed 14 March 2001.

_____. *Annual Polygraph Report to Congress, Fiscal Year 1999*. URL: <<http://fas.org/sgp/othergov/polygraph/dod-1999.html>>. Accessed 14 March 2001.

_____. *Annual Polygraph Report to Congress, Fiscal Year 2000*. URL: <<http://fas.org/sgp/othergov/polygraph/dod-2000.html>>. Accessed 14 March 2001.

_____. *Final Report on the Verification Inspection of the National Security Agency*. Washington DC: GPO, 1996. IR 96-03.

- _____. *Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices*. Washington, DC: GPO, 1985.
- Doyle, Kate. "The End of Secrecy: U.S. National Security and the Imperative for Openness." *World Policy Journal* 16, no 1 (Spring 1999): 34-51
- Eternal Vigilance? 50 Years of the CIA*. Eds. Rhodri Jeffreys-Jones and Christopher Andrew. Portland Or: Frank Cass, 1997.
- Felton, Eric. *The Ruling Class: Inside the Imperial Congress*. Washington DC: Regency Gateway, 1993.
- Ford, Harold P. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*. Lanham, MD: University Press of America, 1993.
- Freedom at Risk: Secrecy, Censorship, and Repression in the 1980s*. Ed. Richard O. Curry. Philadelphia PA: Temple University Press, 1988.
- Freedom of Information Act of 1967*. 5 U. S.Code § 552 (1967).
- Foreign Intelligence Surveillance Act of 1978*. Public Law 95-511, 95th Congress.
- Gertz, Bill. "Ex-CIA Chief Compromised Secrets." *The Washington Times*, 12 October 2000, A1.
- Gill, Peter. "Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community." *Intelligence and National Security* 11, no. 2 (April 1996): 313-331.
- Goodman, Allan E. "The Future of US Intelligence." *Intelligence and National Security* 11, no. 4 (October 1996): 645-656.
- Goodman, Allen E. and Bruce D. Berkowitz. "Intelligence Without the Cold War." *Intelligence and National Security* 9, no. 2 (April 1994): 301-319.
- Gore, Albert. *Common Sense Government - Works Better and Costs Less*. New York: Random House, 1995.
- _____. *The Gore Report on Reinventing Government*. New York: Random House, 1993.
- Hager, Nicky. *Secret Powers: New Zealand's Role in the International Spy Network*. Nelson, N.Z.: Craig Potton Publishing, 1996.

Hannant, Larry. "Inter-war Security Screening in Britain, The United States and Canada." *Intelligence and National Security* 6, no. 4 (1991): 711-735.

Herodotus. *The Histories*. Baltimore Md.: Penguin Books Ltd., 1964.

Hersh, Seymour M. *The Target is Destroyed*. New York: Random House, 1986.

Holden-Rhodes, J.E. *Sharing the Secrets: Open Source Intelligence and the War on Drugs*. Westport, CT: Praeger, 1997.

Hood, William. *Mole*. New York: W.W. Norton and Co, 1982.

The Impact of Intelligence on the Policy Review and Decision-Making Process. Eds. Arthur S. Hulnick and Deborah Brommer. Washington DC: Center for the Study of Intelligence, CIA, 1980.

The Independent Commission on Disarmament and Security Issues. *Common Security: A Blueprint for Survival*. New York: Simon and Schuster, 1982.

Information Security Handbook. Eds. William Caelli, Dennis Longley, Michael Shain. New York: Stockton Press, 1991.

Intelligence and International Relations 1900-1945. Eds. Christopher Andrew and Jeremy Noakes. Exeter, UK: Exeter University Publications, 1987.

Intelligence Security Oversight Office. *Annual Report to the President. Fiscal Year 1979*. Washington DC, GPO, 1980.

_____. *Annual Report to the President 1980-1981*. Washington DC, GPO, 1981.

_____. *Annual Report to the President FY 1982*. Washington DC, GPO, 1983.

_____. *Annual Report to the President FY 1983*. Washington DC, GPO, 1984.

_____. *Annual Report to the President FY 1984*. Washington DC, GPO, 1985.

_____. *Annual Report to the President FY 1985*. Washington DC, GPO, 1986.

_____. *Annual Report to the President FY 1986*. Washington DC, GPO, 1987.

_____. *Annual Report to the President FY 1987*. Washington DC, GPO, 1988.

_____. *Annual Report to the President FY 1988*. Washington DC, GPO, 1989.

_____. *1989 Report to the President*. Washington DC, GPO, 1990.

- _____. *1990 Report to the President*. Washington DC, GPO, 1991.
- _____. *1991 Report to the President*. Washington DC, GPO, 1992.
- _____. *1992 Report to the President*. Washington DC, GPO, 1993.
- _____. *1993 Report to the President*. Washington DC, GPO, 1994.
- _____. *1994 Report to the President*. Washington DC, GPO, 1995.
- _____. *1995 Report to the President*. Washington DC, GPO, 1996.
- _____. *1996 Report to the President*. Washington DC, GPO, 1997.
- _____. *1997 Report to the President*. Washington DC, GPO, 1998.
- _____. *1998 Report to the President*. Washington DC, GPO, 1999.
- _____. *1999 Report to the President*. Washington DC, GPO, 2000.

Intelligence Policy and Process. Eds. Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle. Boulder CO: Westview Press, 1985.

Interagency Classification Review Committee. *Progress Report: Implementation of Executive Order 11652 on Classification, Declassification and Safeguarding National Security Information*. March 31, 1973. Washington DC, GPO, 1973.

_____. *Progress Report: Implementation of Executive Order 11652 on Classification, Declassification and Safeguarding National Security Information*. April 1974. Washington DC, GPO, 1974.

_____. *Progress Report: Implementation of Executive Order 11652 on Classification, Declassification and Safeguarding National Security Information*. May 1975. Washington DC, GPO, 1975.

_____. *1975 Progress Report: Implementation of Executive Order 11652 on Classification, Declassification and Safeguarding National Security Information*. May 1976. Washington DC, GPO, 1976.

_____. *1976 Progress Report: Implementation of Executive Order 11652 on Classification, Declassification and Safeguarding National Security Information*. Washington DC, GPO, 1977.

Jackson, William H. Jr. "Congressional Oversight of Intelligence: Search for a Framework." *Intelligence and National Security* 5, no. 3 (July 1990): 113-148.

- Jeffreys-Jones, Rhodri. "Why Was the CIA Established in 1947?" *Intelligence and National Security* 12, no. 1 (January 1997): 21-40.
- Joint Security Commission. *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence*. Washington DC, 28 February 1994.
- Johnson, Loch K. "Making the Intelligence 'Cycle' Work." *Intelligence and National Security* 1, no. 4 (1986): 1-28.
- _____. *America's Secret Power: The CIA in a Democratic Society*. NY: Oxford University Press, 1989.
- _____. *Secret Agencies: US Intelligence in a Hostile World*. New Haven CT: Yale University Press, 1996.
- _____. "Analysis for a New Age." *Intelligence and National Security* 11, no. 4 (October 1996): 657-671.
- _____. "The CIA and the Question of Accountability." *Intelligence and National Security* 12, no. 1 (January 1997): 178-200.
- Johnson, William R. "The Ambivalent Polygraph." *Intelligence and National Security* 1, no. 3 (1986): 71-83.
- Jordan, Amos A., William J Taylor Jr., and Lawrence J. Korb. *American National Security: Policy and Process*. 4th ed. Baltimore MD: The Johns Hopkins University Press, 1993.
- Kahn, David. *The Codebreakers: The Story of Secret Writing*. New York: Macmillan Publishing Co., 1967.
- Katz, Steven L. *Government Secrecy: Decisions Without Democracy*. Washington DC: People for the American Way, 1987.
- Kennan, George E. *At a Century's Ending*. New York: W.W. Norton and Co., 1996.
- Kent, Sherman. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press, 1949.
- Kessler, Ronald. *Inside the CIA*. New York: Pocket Books, 1992.
- _____. *Moscow Station*. New York: Charles Scribner and Sons, 1989.
- Kirkpatrick, Lyman B. Jr. *The U.S. Intelligence Community: Foreign Policy and Domestic Activities*. New York: Hill and Wang, 1973.

- Knott, Stephen. "Executive Power and the Control of American Intelligence." *Intelligence and National Security* 13, no. 2 (Summer 1998): 171-176.
- Kofsky, Frank. *Harry S. Truman and the War Scare of 1948*. New York: St. Martin's Press, 1993.
- Koehler, John O. *Stasi*. Boulder CO: Westview Press, 1989.
- "The Board Meets in Private, But Is It Legal?" *GovExec.com* April 1996 URL: <<http://www.govexec.com/drcndoc/0496/04963431.html>>. Accessed 31 December 1998.
- Lardner, Richard. "Behind Closed Doors." *GovExec.com* April 1996 URL: <<http://www.govexec.com>>. Accessed 27 December 1999.
- _____. "Keeping Secrets." *GovExec.com*, March 1998, URL: <<http://www.govexec.com>>. Accessed 27 December 1999.
- Laqueur, Walter. *A World of Secrets: The Uses and Limits of Intelligence*. NY: Basic Books, Inc., 1985.
- Lipset, Seymour Martin. "George Washington and the Founding of Democracy." *Journal of Democracy* 9, no. 4 (October 1998): 24-38.
- Lowenthal, Mark M. *US Intelligence: Evolution and Anatomy*. NY: Praeger Publishers, 1984.
- _____. "Searching for National Intelligence: US Intelligence and Policy Before the Second World War." *Intelligence and National Security* 6, no. 4 (1991): 736-749.
- Martin, Frederick Thomas. *Top Secret Intranet*. Upper Saddle NJ: Prentice Hall PTR, 1999.
- Mee, Charles L. Jr. *Playing God*. New York: Simon and Schuster, 1993.
- Mendelson, Kenneth A., Stephen T. Walker, and Joan D. Winston. "The Evolution of Recent Cryptographic Policy in the United States." *Cryptologia* 22, no. 3 (July 1998): 193-210.
- The Military Intelligence Community*. Eds. Gerald W Hopple and Bruce W Watson. Boulder CO: Westview Press Inc, 1986.
- Munson, Richard. *The Cardinals of Capitol Hill: The Men and Women Who Control Government Spending*. New York: Grove Press, 1993.

Mount, Ellis and Wilda B. Newman. *Top Secret Trade Secret*. New York: Neal-Schuman Publishers, Inc., 1985.

Moynihan, Daniel Patrick. *On the Law of Nations*. Cambridge MA; Harvard University Press, 1990.

_____. *Secrecy*. New Haven CT: Yale University Press, 1998.

_____. Senator (D-NY). "The Government Secrecy Reform Act" *Congressional Record*. (19 January 1999) URL: <<http://www.fas.org/sgp/congress/s22.html>>. Accessed 20 March 1999.

National Security Act of 1947. 26 July 1947.

National Security Decision Directive 84. "Safeguarding National Security Information." 11 March 1983.

National Security Institute. *Executive's Security Policy and Procedures Manual*. 3rd Ed. Framington, MA: National Security Institute 1991.

900,000 Await Security Clearances." *The Arizona Republic*. 22 April 2000. A6.

Olvey, Lee D., James R. Golden, and Robert C. Kelly. *The Economics of National Security*. Garden City Park, NY: Avery Publishing Group Inc., 1984.

Oseth, John M. *Regulating U.S. Intelligence Operations*. Lexington KY: The University of Lexington Press, 1985.

O'Toole, G. J. A. *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action From the American Revolution to the CIA*. New York: The Atlantic Monthly Press, 1991.

Pincher, Chapman. *Traitors*. New York: Saint Martin's Press, 1987.

Porch, Douglas. *The French Secret Services*. New York: Farrar, Straus, and Giroux, 1995.

Powers, Thomas. *The Man Who Kept the Secrets: Richard Helms and the CIA*. New York: Alfred Knopf, 1979.

Privacy Act of 1980. 5 U.S. Code § 552a (1980).

Quist, Arvin S. *Security Classification of Information*. Vol. 1, on-line edition, Oak Ridge National Laboratory, 1989. URL: <<http://www.fas.org/sgp/library/quist/index.html>>. Accessed 14 March 2001.

- _____. *Security Classification of Information*. Vol. 2, on-line edition, Oak Ridge National Laboratory, 1993. URL: <<http://www.fas.org/sgp/library/quist/index.html>>. Accessed 14 March 2001.
- Ranelagh, John. *The Agency: The Rise and Decline of the CIA*. New York: Simon and Schuster, 1986.
- Ransom, Harry Howe. *The Intelligence Establishment*. Cambridge MA: Harvard University Press, 1970.
- Richelson, Jeffrey T and Desmond Ball. *The Ties That Bind*. 2nd Ed. Cambridge, MA: Unwin Hyman Inc., 1990.
- Robertson, K.G. "Recent Reform of Intelligence in the UK: Democratization or Risk Management?" *Intelligence and National Security* 13, no. 2 (Summer 1998): 144-158.
- The Role of American Intelligence Organizations*. Ed. George Wittman. New York: The H. W. Wilson Co., 1976.
- Roskin, Michael and Nicholas Berry. *An Introduction to International Relations*. Englewood Cliffs, NJ: Prentice Hall, 1990.
- Secrecy and Foreign Policy*. Eds. Thomas M. Franck and Edward Weisband. New York: Oxford University Press, 1974.
- Select Committee to Study Government Operations. *Final Report, Foreign and Military Intelligence*. Washington DC, 26 April 1976.
- The Seven Military Classics of Ancient China*. Ed. Ralph D. Sawyer. Boulder CO: Westview Press Inc, 1993.
- Smith, Bradley F. "The American Road to Central Intelligence." *Intelligence and National Security* 12, no. 1 (January 1997): 1-20.
- Solomon, Gerald B. *The NATO Enlargement Debate, 1990-1997*. Westport CT: Praeger, 1998.
- Stent, Angela E. *Russia and Germany Reborn*. Princeton, NJ: Princeton University Press, 1999.
- Thomas, Stafford T. *The U.S. Intelligence Community*. Lanham, MD: University Press of America, 1983.
- United States Articles of Confederation*, Art. IX.

United States Congress, Committee on Governmental Affairs. *Report on the Government Secrecy Reform Act of 1998*. 105th Cong., 2d sess., 1998 URL: <<http://www.fas.org/spp/congresssrept238.html>>. Accessed 29 January 1999.

_____. Senate. *Government Secrecy Reform Act of 1998, as amended*. 105th Cong., 2nd sess., 1998. S. 712.

_____. Senate. *Government Secrecy Reform Act of 1999*. 106th Cong., 1st sess., 1999. S. 99.

United States Constitution, Art.1, sec. 5.

United States President. Executive Order 9621. "Termination of the Office of Strategic Services And Disposition of Its Functions." 30 September 1945.

_____. Executive Order 11905. "United States Foreign Intelligence Activities." 18 February 1976.

_____. Executive Order 12036. "United States Intelligence Activities." 24 January 1978.

_____. Executive Order 12333. "United States Intelligence Activities." 4 December 1981.

_____. Executive Order 12334. "President's Intelligence Oversight Board." 4 December 1981.

_____. Executive Order 12356. "National Security Information." 1 April 1982.

_____. Executive Order 12537. "President's Foreign Intelligence Advisory Board." 28 October 1985.

_____. Executive Order 12575. "President's Special Review Board." 1 December 1986.

_____. Executive Order 12958. "Classified National Security Information." 17 April 1995.

_____. Executive Order 12968. "Access to Classified Information." 4 August 1995.

_____. Military Order. "Office of Strategic Services." 13 June 1942.

_____. Presidential Order. "Coordinator of Information." 11 July 1941.

_____. Presidential Order. "Coordination of Federal Foreign Intelligence

Activities.” 22 January 1946.

Vest, Jason and Wayne Madsen. “A Most Unusual Collection Agency.” *The Village Voice* 24 February 1999. URL: <<http://www.jya.com/nsa-scs.html>>. Accessed 20 March 1999.

West, Nigel. *Games of Intelligence: The Classified Conflict of International Espionage*. New York: Crown Publishers, 1989.

_____. *The SIGINT Secrets*. NY: William Morrow and Co., 1986.

Whitaker, Reg. “The Politics of Security Intelligence Policy-making in Canada: I 1970-84.” *Intelligence and National Security* 6, no. 4 (1991): 649-668.

_____. “The Politics of Security Intelligence Policy-making in Canada: II 1984-91.” *Intelligence and National Security* 7, no. 2 (1992): 53-76.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford CA: Stanford University Press, 1962.

Woodward, Bob. *Veil: The Secret Wars of the CIA*. New York: Simon and Schuster, 1987.

Zimmerman, David. *Top Secret Exchange: the Tizard Mission and the Scientific War*. Buffalo, NY: McGill-Queen’s University Press, 1996.