I Overview: Protecting Secrets and Reducing Secrecy

Commission Purposes and Objectives

Congress established the Commission on Protecting and Reducing Government Secrecy in Title IX of the Foreign Relations Authorization Act for Fiscal Years 1994 and 1995 (Public Law 103-236) to make "comprehensive proposals for reform" that are designed "to reduce the volume of information classified and thereby to strengthen the protection of legitimately classified information," as well as to improve existing personnel security procedures. In meeting these objectives, the Commission seeks to promote both the effective protection of information where warranted and the disclosure of information where there is not a well-founded basis for protection or where the costs of maintaining a secret outweigh the benefits.

From the beginning of the American republic, and especially over the past half century, a tension has existed between the legitimate interest of the public in being kept informed about the activities of its Government and the legitimate interest of the Government in certain circumstances in withholding information; in short, between openness and secrecy. This report analyzes the grounds for this tension and suggests means for reconciling the dual "protecting" and "reducing" objectives that are part of the Commission's name and authorizing statute.

It is essential to define the appropriate spheres of protecting and reducing secrecy to avoid perpetuating a system that was identified more than forty years ago as "so overloaded that proper protection of information which should be protected has suffered" and one in which "the mass of classified papers has inevitably resulted in a casual attitude toward classified information, at least on the part of many."[1] The challenge of reducing secrecy overall and protecting secrets more effectively has increased since that time with the broadening reach of national security concerns. Even as the Freedom of Information Act (FOIA) has created a means for the public to obtain government information, consistent with security requirements, the reach of government secrecy has expanded in line with broadened conceptions of what must be protected in the name of national security. Moreover, although the current executive order on classification places a greater burden on those who seek to classify information, existing incentives still tend to promote secrecy over openness.

The result today is a system which neither protects nor releases national security information particularly well. Substantial concerns exist with respect to both the ability of the classification system to protect secrets effectively and the adequacy of the procedures in place to make information available to those outside the Government. In part, this is because the protection of government secrets and the reduction of government secrecy too often have been viewed as competing objectives, instead of being seen as able to reinforce one another when practiced effectively.

This Commission is the first body established by Congress to examine government secrecy in four decades. The only prior body created by statute, the Commission on Government Security, was established in 1955 and issued its final report in 1957. Other commissions and task forces have examined elements of the security system; the most significant of these are described in Appendix G. Some of these previous bodies concluded that incremental changes to the classification system and other security procedures would suffice, while others—most notably the Seitz Task Force of the Defense Science Board in 1970—proposed broader reforms. Several also addressed the problems that arise from inadequate protection of classified information by government officials.

In each case, however, any changes that followed did not alter significantly the basic structure and underpinnings of the security system that developed primarily during the early years of the Cold War. (Although implementation of the recommendations made three years ago by the Joint Security Commission is still an ongoing process, most of the changes made concern specific security practices and procedures; they have little consequence for those outside of government, aside from industrial contractors, and have not affected the functioning of the system overall.)

Indeed, the central finding of the Commission on Government Security that there existed a "vast, intricate, confusing and costly complex of temporary, inadequate, uncoordinated programs and measures designed to protect secrets and installations vital to the defense of the Nation against agents of Soviet imperialism" still rings true today. Many of those programs and measures have proven to be anything but "temporary," however, remaining in place even as the overarching threat to U.S. security posed by the Soviet Union and its ideological supporters within the United States dissipated and gave way to a new set of very different and less monolithic security challenges. To a significant degree, and despite the various studies and a succession of executive orders on classification, today's system remains deeply rooted in the concepts and principles examined thoroughly by the Commission on Government Security four decades ago.

This is particularly striking in view of the National Security Agency's release, beginning in July 1995, of the VENONA intercepts describing Soviet espionage in the United States during the 1940s. Those documents provide historians with a new opportunity to analyze the Commission on Government Security's conclusion that "the Communist threat is both real and formidable." They also reveal how far the United States has come from an era of espionage activities based mainly on ideological motives. Yet even as the global Communist threat is now being analyzed as a historical phenomenon, the security classification and personnel security system that grew up largely in response to it has yet to adapt to new realities.

The revolution in information technology, which has changed the landscape of how the government creates, manages, and protects its information, accentuates this failure of the system to adapt. The estimation that the amount of available information in the United States will grow nineteen times between 1992 and 2000 highlights both the opportunities and the challenges in the years to come.[2] The United States possesses the world's most highly connected and at the same time most vulnerable information infrastructure; a denial or disruption of service could have a significant negative

impact, not only on the protection of classified national security information, but more broadly on the functioning and credibility of the Federal Government as a whole.

Moreover, as more records are created and distributed electronically, it will be essential to focus additional attention on how to prevent information from being manipulated or modified in a manner that would alter its basic content or render it unavailable—problems that were much less likely to arise in a "paper-based" world. In light of these varied new challenges, this report also describes key information security issues which relate to both the "protecting" and the "reducing" elements of the Commission's charter.

Secrecy Issues Not Addressed by the Commission

In view of the breadth of its title, the Commission also had to decide which issues relating to government secrecy *not* to address. First, the Commission did not try to examine every facet of the security system. For example, the report does not discuss the myriad of physical and technical security measures used to safeguard information, ranging from facilities protection to document control to operations security requirements. Many of these were addressed in the Joint Security Commission's 1994 report and several of the changes recommended in that report have since been reviewed within the interagency Security Policy Board structure (although the implementation record to date has been mixed).

Nor does this report detail how secrecy is maintained in the Legislative and Judicial Branches (for example, through secrecy oaths and disclosure orders), except in areas that relate to the classification, declassification, personnel security, and information systems security criteria and procedures developed by the Executive Branch. The report also does not examine the impact of various government security requirements on the private sector—including patent, trade secret, and other invention secrecy rules, and export control laws and regulations—except where they relate directly to the protection of *government* secrets.

The Commission also does not address certain issues that, while obviously related to government secrecy, are best considered in the context of a broader examination of intelligence roles and missions. Thus, the appropriate status of the U.S. intelligence budget, role and conduct of covert actions, procedures for intelligence sharing with allies and international organizations, and relationship between intelligence and law enforcement objectives are not addressed in this report. These were among the matters reviewed in the past year by the Commission on the Roles and Capabilities of the United States Intelligence Community in its report, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, by task forces on intelligence reform organized by the Council on Foreign Relations and Twentieth Century Fund, and in the report of the House Permanent Select Committee on Intelligence, *IC21: Intelligence Community in the 21st Century*. This Commission has explored government secrecy by analyzing the basic policies and procedures through which it is developed and maintained—not by examining particular secret operations.

Finally, the Commission has drawn a distinction between "secrecy" and "privacy." In *The Torment of Secrecy* (originally published in 1956 and reissued last year with an Introduction by Chairman Moynihan), Edward A. Shils contrasted "secrecy," which he defined as "the compulsory withholding of knowledge, reinforced by the prospect of sanctions for disclosure," from "privacy," which he termed "the voluntary withholding of information reinforced by a willing indifference."[3] The report does not analyze the requirements of the Privacy Act of 1974 nor evaluate the balancing of governmental policies and individual rights, although it does cite privacy interests in discussing subjects such as personnel security procedures and the difficult effort to attempt to develop an updated encryption standard.

Defining Government Secrecy

Scholars have struggled with the general concept of secrecy for centuries. Philosopher and ethicist Sissela Bok has defined a secret as anything that "is kept intentionally hidden, set apart in the mind of its keeper as requiring concealment."[4] A secret may either be kept from everyone or shared on the condition that it go no further. The key element is intentional concealment: the action by one or more "insiders" of keeping something hidden and set apart from any "outsiders." Secrecy is, in turn, the resulting concealment. Edward Shils's definition of secrecy, cited above, adds the element of "sanctions for disclosure" to the framework. As discussed below, however, one of the fundamental problems over the past few decades has been the absence of any clear relationship between the rules for keeping secrets through classification and those for imposing effective discipline when the established safeguards are breached.

> "Three may keep a secret if two of them are dead."
>
> Benjamin Franklin

There is nothing particularly unique about the general means by which the U.S. Government seeks to ensure effective protection of its secrets. The process rests on three pillars. First, an official must identify what information is to be kept secret and then the means for maximizing the likelihood that it will remain secret; in short, the rules for classification and physical security. As the universe of those with whom the information is communicated increases, however, so does the likelihood of an unwanted disclosure. Thus, the second pillar of effective secrecy is to ensure that the secret is shared only with those viewed as trustworthy: a combination of personnel security rules and the principle of "need-to-know." Finally, as Shils's definition reflects, there is a third pillar: rules that those who breach the commitment to maintain secrecy will be subject to some type of sanction. In the context of protecting national security information, this means enforcement through the espionage laws as well as through applicable administrative procedures.

Where any one of these pillars is weak or otherwise not utilized effectively, the secrecy system is not likely to function well. Moreover, the inadequacy of one element may well lead those responsible for the system's administration and management to "compensate" by expanding application of the other pillars. Thus, the perception that the system of sanctions for violating the rules for protecting information is ineffective may contribute to a tightening of the other measures intended to provide security: namely, the rules governing personnel security and classification.

The Means for Protecting Government Secrets

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. Of these, the first two categories together define the sphere of "national security information" covered by security classification executive orders and are the primary subjects of this Commission's inquiry.

The U.S. Constitution includes only one explicit reference to "secrecy," and it concerns procedures of the Congress, not the Executive Branch. Article I, section 5 provides "Each House shall keep a journal of its Proceedings, and from time to time publish the same, excepting such Parts as in their Judgment require Secrecy." The authority of the Executive Branch to maintain secrecy has been based in part on four statutes: the Espionage Act, the National Security Act, the Atomic Energy Act, and the Freedom of Information Act.

Nevertheless, as it has developed in the United States over the past eight decades, government secrecy can be understood best 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."

The series of six executive orders since 1951, however, does not represent the full range of secrets protected through some form of regulation. A great deal of information is protected by the Government *outside* the formal national security classification system. One especially confounding matter has been the uncertain scope of "sensitive unclassified information": information not meeting the criteria for classification but that is considered by the Government to warrant some form of protection. This category (or, more accurately, categories) of information has remained difficult to define, in part because of the greatly varied rationales used to justify its protection.

In 1971, a House subcommittee found no fewer than 62 different control markings being used to restrict the distribution of sensitive unclassified information. Use of these markings was not linked to any explicit statutory authority. In fact, unlike the tiers of Confidential, Secret, and Top Secret security classification, they also were not expressly authorized by executive order. The Commission's own inquiry reveals that,

while certain markings have been eliminated and others narrowed since 1971, in most respects little has changed. The numerous markings—more than 50—still used today continue to produce considerable confusion both inside and outside the Government. Chapter II discusses this issue of sensitive unclassified information in greater detail.

The Importance of Protecting Secrets

Effective secrecy has proven indispensable to the functioning of government, serving the interests not only of the officials in power but of the governed as well. Secrecy permits policymakers to freely explore and debate different options, consider alternatives, and weigh the consequences of each; aids in providing the critical element of surprise with respect to a chosen policy; and protects individuals from the possible harm that could arise from publicity.

The primary objective of government secrecy in the national security realm, including its application through the classification system, is to protect U.S. interests by controlling information that provides an advantage (including the element of surprise) over an adversary or prevents that adversary from gaining an advantage that could damage the United States. As the Senate Select Committee on Intelligence noted in its 1986 report reviewing U.S. counterintelligence and security programs, the main rationale underlying classification of national security information must be to ensure that "a hostile element whose goal is to damage the interests of the United States should not have use of the information."[5]

The maintenance of secrecy has proven essential to the successful development, implementation, and completion (or, conversely, the abandonment) of plans and missions. World War II affords several notable examples of successful secrecy in protecting key cryptologic programs from the Germans and the Japanese. (Most of the more recent examples of successful secrecy during wartime remain classified, making it difficult to cite more contemporary cases of such successes.) Secrecy obviously is essential in maintaining the element of surprise that is so critical to the success of particular military missions.

The successful conduct of plans and missions in turn may depend on protecting key technologies. A notable success in this regard was the protection of the efforts, beginning in the 1950s, at Lockheed's Skunk Works facility to rapidly develop an aircraft capable of providing reliable intelligence on Soviet activities. That facility came to be seen as a model for its successful protection of several highly classified aircraft development programs in the years that followed.[6]

Secrecy also is essential to the effective conduct of diplomatic negotiations. The secret diplomacy that preceded President Nixon's trip to China in 1972 provides one well-known example of how secrecy was maintained successfully with regard to a major diplomatic undertaking. More routinely, preserving the secrecy of the specific elements of ongoing negotiations is regarded as essential to their ultimate success.

Closely linked to the protection of plans and missions and the conduct of diplomatic negotiations is the protection of internal policy deliberations: the negotiations among

government officials that precede and accompany the development of the plans, missions, and external negotiations cited above. Policy often is shaped only gradually, and the process of developing a coherent official government position often is marked by long periods of disagreement and conflict. Indeed, in *Federalist No. 64*, John Jay cited "preparatory and auxiliary measures" relating to negotiations as the matters that "usually require the most secrecy and the most dispatch."[7]

As one scholar has noted:

> If administrators had to do everything in the open, they might be forced to express only safe and uncontroversial views, and thus to bypass creative or still tentative ideas. As a result, they might end by assuming hasty and inadequate positions. Chances to learn might be lost; premature closure with respect to difficult issues would become more likely. In order to create a pattern out of chaos and avoid haphazard choices, administrators must be able to consider and discard a variety of solutions in private before endorsing some of them in public; the process of evolving new policies requires a degree of concealment.[8]

Thus, drafts and memoranda used in negotiations often remain classified even when the final positions and statements do not. Secrecy also may aid those within government who oppose a particular policy. Of course, this is a benefit to the extent that it enables government to function effectively at a given point in time. However, there also are dangers in the continued maintenance of secrecy that "obscures from the public the divisions and dissensions comprising the administrative history of most important Executive decisions," as well as the fact that, when policies end in failure, there may have been "heroes" who opposed them.[9]

Finally, secrecy is essential in protecting confidential relationships with individuals. The protection by the Government of individuals' identities may take several forms and arise in varied contexts, but probably the best known basis for safeguarding confidential relationships is that enshrined in the National Security Act of 1947 concerning the protection of intelligence sources and methods. This rationale for protection is based primarily on the concern that revealing identities would present substantial risks both to the individuals themselves, to their families, and more broadly to the nation's interests. As evidenced by the actions of Aldrich Ames and other notorious spies, the failure to keep secrets in this context—whether deliberate or unintentional—can have lethal consequences. Moreover, the loss of even a single source in turn may have a chilling effect on the ability to utilize others in the future.

The Intangible Costs of Secrecy

Notwithstanding the compelling interests summarized above, secrecy also carries a range of costs for those responsible for maintaining the secrets and those from whom they are kept. Secrecy has the potential to undermine well-informed judgment by limiting the opportunity for input, review, and criticism, thus allowing individuals and groups to avoid the type of scrutiny that might challenge long-accepted beliefs and

ways of thinking. Some form of "sunlight" that permits views to be challenged while they are still in the formative stage can help reveal any institutional biases or preconceived ideas about how to approach a particular issue.

Related to the above, and particularly relevant in the scientific arena, is the impact when secrecy does not permit the sharing of information on new applications of technology. This was a chief interest of the Task Force on Secrecy, established by the Defense Science Board and chaired by Dr. Frederick Seitz, which found, in its July 1970 report, that as a general matter "the classification of technical information impedes its flow within our own system, and may easily do far more harm than good by stifling critical discussion and review or by engendering frustration."[10]

In addition, the failure to ensure timely access to government information, subject to carefully delineated exceptions, risks leaving the public uninformed of decisions of great consequence. As a result, there may be a heightened degree of cynicism and distrust of government, including in contexts far removed from the area in which the secrecy was maintained.

Secrecy can also have significant consequences for the functioning of government itself. Information is power, and it is no mystery to government officials that power can be increased through controls on the flow of information.

One persistent problem in this context has been the intermingling of secrecy used to protect carefully defined national interests with secrecy used primarily to enhance such political or bureaucratic power. This creates the potential that some officials, welcoming insulation from outside scrutiny, will seek means to develop and maintain secrecy beyond what is authorized in a statute or regulation. (An example is when sources and methods protection under the National Security Act is used to deny access to information that does not reveal a particular intelligence source or method.) Such actions obviously have significant consequences for relationships between different parts of government.

As the scope of secrecy grows and the system for protecting secrets becomes more layered and complex, the prospect for leaks—deliberate releases of classified information, nearly always on an anonymous basis—grows as well. Secrets become vulnerable to betrayal, often from high in the chain of command; this in turn promotes greater disrespect for the system itself. Those condemning leaks may, at the same time, be using them in their own self-interest for any number of reasons (ranging from the desire to gain a bureaucratic advantage to using leaks as "trial balloons" for possible policy initiatives). The anonymous leak, often at a senior level, "has become an important tool of governing" and a form of "instant declassification" (although the information leaked is likely to remain officially classified notwithstanding its publication).[11]

> "Leaking has a symbiotic relationship with secrecy. Without secrecy there would be no need to leak information. As government secrecy grows and comes to involve more people, the opportunities to leak from within expand; and with increased leaking, governments intensify their efforts to shore up secrecy."
>
> Sissela Bok, *Secrets*

The leaking of secrets has important consequences for the quality of information made available to the public, as well as for the ability to verify the information. Leaking creates a double standard that may, at times, pit political and career government officials against one another. To the extent that leaking gains any legitimacy, it complicates efforts to impose sanctions on officials for overclassification or other abuses of classification. Leaks that result in changes in policy would appear to reward those within the Government whose motivations may be the most dubious—not those interested in a more sustained and consistent approach to promoting greater openness. Finally, and perhaps most importantly, leaking can greatly damage the integrity of and public respect for the overall classification system, including those efforts by the Government to control the information that is most vital to the nation's security. Leaks undermine the credibility of classification policies and other restrictions on access to information, making it harder to differentiate between secrecy that is needed to protect highly sensitive national security information and that which is not well-founded.

Efforts to Quantify the Costs of Secrecy

Understanding the financial costs associated with keeping information secret is essential to any effort to begin scaling back the scope of secrecy and making protection more efficient. Efforts to measure the costs of classification and related security measures have increased significantly in the past three years. While the U.S. General Accounting Office (GAO) first attempted to measure such costs in a 1972 study and issued a second report in 1993 on the costs "directly applicable to national security information," the Joint Security Commission in 1994 described security costs as "an elusive target" for which there was not a coordinated approach to a uniform cost accounting methodology.[12]

Today, the Government and industry still are not well-positioned to analyze the cost data collected in order to make better-informed decisions on allocating resources. However, progress has been made in quantifying at least the overt costs of classification and related security measures. This has occurred primarily as a result of two surveys mandated by the Congress and carried out under Office of Management and Budget (OMB) guidance, in which Federal agencies have reported on their "classification-related" security costs. The surveys focused on the costs associated with the protection of classified information, and did not include costs related to unclassified information considered to be sensitive, nor costs for the protection of proprietary business information, property, and other assets, nor costs for counterintelligence activities. In addition, declassification costs are not listed separately.

The first survey, released in April 1994, estimated the total security costs of reporting agencies and departments for the preceding year at approximately $2.27 billion; the classified submission of the Central Intelligence Agency (CIA) was not included. A second cost survey was developed in 1995, with a better defined set of reporting categories; issued in April 1996, it reported total security classification costs of roughly $2.7 billion annually for Fiscal Year 1995 and Fiscal Year 1996. As in the earlier survey, the CIA did not provide its cost data in unclassified form.

Efforts to quantify security costs in industry have proceeded more sporadically since a 1989 Aerospace Industries Association (AIA) survey reported $13.8 billion in industry costs (extrapolating from data submitted by fourteen large firms) relating to the protection of national security information. Under Executive Order 12829 of January 1993, which established the National Industrial Security Program (NISP), the Information Security Oversight Office (ISOO) must report to the President on the costs associated with the NISP's implementation. However, there has been considerable debate on the proper approach to accounting for industry costs, and industry has shown reluctance to collect such information.

In 1995, government and industry officials jointly developed a one-page "data collection worksheet" on estimated industry costs. The data submitted in June 1996 estimated, based on a sample of 23 companies, total industry costs relating to protecting national security information for 1995 of more than $2.9 billion. Thus, taking the most recent government and industry cost estimates together, over $5.6 billion was spent in 1995 to protect classified national security information.

The Commission strongly endorses the efforts to attempt to quantify the costs of secrecy. Considerable progress already has been made in a short time in calculating the costs of security classification, and the Commission urges the continued development and refinement of methodologies to help determine these costs, as well as to better calculate the costs of different methods of declassifying information. At the same time, the Commission notes that even these improved cost accounting efforts do not attempt to measure the various intangible costs associated with classification and related activities. Such costs are difficult, if not impossible, to quantify with any degree of precision, yet they must be taken into account in any meaningful evaluation of the secrecy system.

Evolving Concepts of National Security

Under the series of executive orders that have been the cornerstone of the Government's information protection system over the past half century, the concept of national security has formed the basis for classifying information. In practice, however, the breadth of the definition—first referenced in the 1951 Truman Order and then reintroduced in the 1972 Nixon Order—has left those holding the "classification stamp" with great flexibility to decide what national security means in a given context.[13]

Over the years, various government officials and scholars have attempted to provide a theoretical underpinning to national security. Professor Arnold Wolfers, writing in the 1940s and 1950s, produced a framework for viewing it as "the ability of a nation to protect its internal values from external threats," but this definition still left a great deal of leeway for interpreting just what the relevant "internal values" actually are.[14] Are they, for example, limited to the defense sphere and primarily the maintenance of military strength? If so, then why the prevailing use of the term "national security" rather than the narrower "national defense" generally used earlier, including in the espionage laws? Do "internal values" also encompass the ability to maintain an

advantageous foreign relations position? To sustain a productive domestic economy? To protect the environment (a matter of growing national and international concern)?

What seems clear is that, given the realities of modern government, with an increasingly complex relationship between matters of defense, foreign policy, and economic policy, and with the expansion of the subject areas considered important to the protection of U.S. national interests, the concept of national security now ranges well beyond the traditional military dimension alone. The President, the Congress, and other senior officials are likely to regard a broad range of matters as directly relevant to the country's security.

This is not to suggest that the expanded framing of national security alone can explain the growth of government secrecy over the past half century. Indeed, it is far from clear that working-level classifiers even consider the meaning of the underlying term "national security," as opposed to simply trying to fit particular information into one of the categories of the applicable classification order. Still, the scope of the term does have implications both for what officials can be expected to treat as classified and for the distinctions drawn between the categories of information deemed to require classification, information protected in other ways, and information not subject to any form of governmental protection.

A Statutory Basis for the Secrecy System

The Case for a Statutory Approach

Many of the problems described in the following chapters, particularly the poor record of implementing classification and declassification policies, derive from the absence of a stable and consistent classification regime. The classification system has been subjected to six different executive orders since 1951, four of which have been issued in the last quarter century alone.

The rules governing how best to protect the nation's secrets, while still ensuring that the American public has access to information on the operations of its government, past and present, have shifted along with political changes in Washington. Over the last 50 years, with the exception of the Kennedy Administration, a new executive order on classification was issued each time one of the political parties regained control of the Executive Branch. These have often been at variance with one another both with respect to the front-end process for classifying and the back-end process for declassifying—at times even reversing outright the policies of the previous order.

As a result, the classification system has undergone repeated adjustments (and, in some cases, major shifts in emphasis) without corresponding improvements in effectiveness. The three executive orders issued since 1978 highlight the problem. As discussed in Chapter II, in many ways President Clinton's Executive Order 12958 closely resembles President Carter's Executive Order 12065—following a thirteen-year interval under President Reagan's Executive Order 12356, which differed from the other two in significant ways. The classification policies of today are similar, in

several respects, to what they were in 1978. So are many of the basic shortcomings of the system that officials were trying to deal with two decades ago.

Repeated changes both disrupt the efficient administration of the classification system and can be very costly. Each new order has required that agencies devote significant time and resources attempting to make personnel aware of how policy changes affect their work. Although the resources needed to implement new policies can be substantial, rarely are the requirements coordinated with the budget process to ensure that adequate funds are allocated. In 1983, officials from the Information Security Oversight Office (ISOO) noted that the "frustration" throughout the Government over having to implement the Reagan Order less than four years after the issuance of the Carter Order was similar to that experienced when the Carter Order replaced President Nixon's Executive Order 11652 after only six years.

The costs of repeated changes will only increase as more documents are prepared and used on electronic media. For example, the high cost of making changes to computer systems, together with the fact that further revisions were expected due to other policy changes, led NSA officials to postpone updating programs to comply with Executive Order 12958 so that all changes could be made simultaneously at a lower overall cost. The result was that well over a year after the Order was issued, nearly every NSA intelligence report reviewed by the Commission was still being issued with the marking "OADR" (Originating Agency's Determination Required), even though that marking had been abolished by the new Order.[15]

Aware that classification orders are regularly replaced, some officials opposed to the specifics of a given order have resisted complying with and enforcing policies, essentially waiting out an administration in the hope that the order will be replaced. For example, the declassification provisions of President Carter's Executive Order 12065 were never fully implemented before being scaled back under Executive Order 12356. This highlights an important shortcoming in the way classification rules currently are issued and carried out.

The process of developing these classification orders also does little to promote a system that encourages a balanced assessment of the need for secrecy. Although there was some opportunity for public comment before the issuance of Executive Order 12065 in 1978 and Executive Order 12958 in 1995, classification orders have been developed to a large extent by agency representatives in venues not open to the public. A senior official involved with one such effort noted that "a group of this kind has a limited perspective" and that there is "no way to bring balance to the process from within the Government because there are no institutional advocates for reform of the classification process within the agencies."[16]

Many of the changes proposed in this report for improving classification and declassification practices probably could be achieved within the current regulatory system. However, past efforts that relied on those inside the Government to change the system from within did not result in significant long-term improvements. A more stable foundation is required for the entire classification and declassification system, with more consistent application of established rules across all agencies that classify and less ability to "opt out" where there is disagreement with particular rules. Providing a

legislative basis for the classification and declassification system offers a much likelier means for achieving these types of meaningful changes.

The statute described below is intended to respond to the numerous concerns raised, both directly with this Commission and in the course of previous examinations of the classification and declassification system, about the absence of a stable, coherent regime. It is designed to promote greater attention by the Congress to the dual interests of reducing secrecy overall and better protecting that which should remain secret, while leaving the day-to-day administration of the system in the hands of the Executive Branch. One intended objective of this heightened scrutiny is development of a clearer understanding of the scope of what should be protected under the security classification system. At the same time, however, the Commission does not view this proposed statute as the vehicle for all of its suggestions for improving the current system; indeed, the implementation of most of the recommendations in Chapters II through V would require only Executive Branch action.

Even so, enactment of this general, overarching statute would have the laudatory effect of increasing the likelihood of oversight and, thereby, of promoting greater accountability on the part of the officials within the Executive Branch responsible for setting policies and making decisions on classification and declassification matters. As noted above, while many of the changes proposed throughout this report could be accomplished even without a new law, adoption of a statute affords the best prospect for developing a new approach to the management of classified national security information—an approach characterized by an improved understanding of how best to reconcile and balance the objectives of protecting secrets and reducing secrecy.

A Proposed Statute

The basic rules governing classification and declassification should be the product of an open discussion that weighs both the advantages and disadvantages of secrecy and that is not restricted to the views of those charged with implementing regulations. The Congress can provide such a forum. In addition, there must be incentives for senior agency officials to comply with established policies, coupled with an expectation that they will be held accountable if they do not. The increased likelihood of oversight by the Congress under a statutory framework would provide such an incentive for senior officials to exert greater leadership to ensure the appropriate use of classification and better protection of classified information. In fact, numerous officials from different agencies acknowledged to the Commission that they would be more likely to implement policies backed by the force of a law passed by the Congress.

Recommendation

The Commission recommends enactment of a statute establishing the principles on which Federal classification and declassification programs are to be based.

The Commission proposes the following as the framework for such a statute:

> Sec. 1 Information shall be classified only if there is a demonstrable need to protect the information in the interests of national security, with the goal of ensuring that classification is kept to an absolute minimum consistent with these interests.*
>
> Sec. 2 The President shall, as needed, establish procedures and structures for classification of information. Procedures and structures shall be established and resources allocated for declassification as a parallel program to classification. Details of these programs and any revisions to them shall be published in the Federal Register and subject to notice and comment procedures.
>
> Sec. 3 In establishing the standards and categories to apply in determining whether information should be or remain classified, such standards and categories shall include consideration of the benefit from public disclosure of the information and weigh it against the need for initial or continued protection under the classification system. If there is significant doubt whether information requires protection, it shall not be classified.
>
> Sec. 4 Information shall remain classified for no longer than ten years, unless the agency specifically recertifies that the particular information requires continued protection based on current risk assessments. All information shall be declassified after 30 years, unless it is shown that demonstrable harm to an individual or to ongoing government activities will result from release. Systematic declassification schedules shall be established. Agencies shall submit annual reports on their classification and declassification programs to the Congress.
>
> Sec. 5 This statute shall not be construed as authority to withhold information from the Congress.
>
> Sec. 6 There shall be established a National Declassification Center to coordinate, implement, and oversee the declassification policies and practices of the Federal Government. The Center shall report annually to the Congress and the President on its activities and on the status of declassification practices by all Federal agencies that use, hold, or create classified information.

* The term "national security" is used in the current classification order (Executive Order 12958, issued by President Clinton in April 1995 and effective in October 1995), as well as in previous classification orders. As Section 2 of the proposed statute makes clear, the President retains the authority and the discretion to determine which categories of information should be open to classification. Nevertheless, having considered this issue in detail, the Commission proposes several categories of information that it believes should be considered for classification. The list of those categories is set out in Chapter II of this report at pages 22-23.

In calling for enactment of a statute, the Commission is aware of the likely difficulties in securing its passage. This is not the first time that a legislative approach to classification management has been advanced, and the fate of past efforts is a testament to the Congress' general reluctance to involve itself in an area often perceived as the exclusive domain of the President. Even so, a half century of near-total deference to the Executive Branch to both design and implement secrecy standards through regulation has resulted in a system that is long overdue for change.

The U.S. Supreme Court has held that the President's authority to "classify and control access to information bearing on national security . . . flows primarily from th[e] constitutional investment of power in the President" as Commander in Chief.[17] At the same time, the Necessary and Proper Clause in Article I, section 8, of the Constitution, which grants the Congress the authority to "make Rules for the Government and Regulation of the land and naval forces," provides a strong basis for Congressional action in this area. As an area in which the President and the Congress "may have concurrent authority, or in which its distribution is uncertain," the security classification system may fall within the "zone of twilight" to which Justice Robert H. Jackson referred in 1952 in his famous concurring opinion in *Youngstown Sheet and Tube v. Sawyer* (the "steel seizure" case).[18]

Moreover, there are clear precedents for Congressional action in this area. In the Atomic Energy Act of 1954, the National Security Act of 1947, and the Assassination Records Collection Act of 1992 (which established broad standards for the declassification of records concerning the assassination of President Kennedy), Congress prescribed standards to govern elements of the classification and declassification process. None of these statutes infringed on the ability of the Executive Branch to administer the classification system, nor have they compromised the ability of agencies to protect sensitive information. In fact, statutory authority for protecting information routinely is cited by agency officials as helping promote sound information management programs. The power of a statute also could assist future administrations in implementing policies on classified information.

Because the proposed statute would provide only the basic principles under which the classification system would operate, it should not raise concerns about separation of powers. The President would retain the authority to implement the law in the manner deemed most appropriate in light of the particular national security concerns existing at the time, as long as such procedures remained within the general boundaries of the law.

Section 1 of the proposed statute provides, consistent with recent executive orders, that classification shall be based upon "interests of national security." Section 2 provides that the President would retain the authority to specify which kinds of information come within the scope of national security. The Commission envisions that the statute also would establish the general procedures governing the declassification of information, consistent with the objective of developing a government-wide "life cycle" approach to the management of classified information. As explained in Chapter III, the statute would include a government-wide program for the declassification of classified information after definite time periods, subject only to specific exemptions. Part of this program would also involve establishment of a

National Declassification Center within an existing agency, most logically the National Archives and Records Administration.

Conclusion

The twelve Commissioners have brought to this inquiry a diverse range of perspectives drawn from varied backgrounds in the Executive and Legislative Branches and in the public and private sectors. Yet despite varied philosophies and work experiences, the Commissioners all agree with the need to change the system in place today for protecting government secrets in response to the dramatic transformations that have occurred since the only prior statutory commission completed its work some four decades ago. New approaches are needed not only because of changing security threats and risks, but also because costs must be contained; while redundancies perhaps could be tolerated in the past, today's realities require much more efficient, prioritized, and cost-effective procedures.

Chapters II through V amplify on the general observations outlined above in the four areas of classification, declassification, personnel security, and information systems security. Each chapter also explores the historical roots of current practices and the consequences for both the dissemination of government information to the public and the sharing of information within the Federal Government. Among the key themes addressed, which transcend the specific findings and recommendations in each chapter, are the functioning of the bureaucracy that has developed over the past half century to protect government secrets; the efforts to promote greater oversight and accountability; and the various costs associated with both protecting secrets and reducing secrecy.

The Commission recognizes the obstacles to achieving substantial improvements, at least in the short term. At the same time, it believes that there now exists a heightened opportunity to propose and build support for changes intended to reduce secrecy and improve the protection of what remains secret. The chapters that follow detail the changes that the Commission recommends to meet both of these objectives.

---

[1] Department of Defense, Committee on Classified Information, *Report to the Secretary of Defense by the Committee on Classified Information* (Washington, D.C.: Department of Defense, 8 November 1956), 6.

[2] Thomas Lipscomb, "*American Competitiveness in the Information Age,*" presentation at the National Policy Forum Conference (Washington, D.C., 25 October 1995), quoting James Billington, the Librarian of Congress.

[3] Edward A. Shils, *The Torment of Secrecy* (Glencoe: The Free Press, 1956, reprint with an Introduction by Daniel Patrick Moynihan, Chicago: Ivan R. Dee, Inc., 1996), 26.

[4] Sissela Bok, *Secrets* (New York: Vintage Books, 1989), 5.

[5] Senate Select Committee on Intelligence, *Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs*, 99th Cong., 2d sess., 1986, Rpt. 99-522, 78.

[6] At the same time, as Lockheed Martin Skunk Works President Jack S. Gordon made clear in a letter and an accompanying "white paper" sent to the Commission on September 18, 1995, the firm worked to ensure that its security practices protected technological capabilities without imposing unnecessary costs or imposing counterproductive restraints on its own officials (Jack S. Gordon, letter to Commission staff, 18 September 1995).

[7] Thomas M. Franck and Edward Weisband, "Dissemblement, Secrecy, and Executive Privilege in the Foreign Relations of Three Democracies: A Comparative Analysis," in *Secrecy and Foreign Policy*, ed. Thomas M. Franck and Edward Weisband (New York: Oxford University Press, 1974), 400-01.

[8] Bok, *Secrets*, 175.

[9] Ibid., 9.

[10] Defense Science Board Task Force on Secrecy, *Report of the Defense Science Board Task Force on Secrecy* (Washington, D.C.: Office of the Director of Defense Research and Engineering, 1 July 1970), 9.

[11] William S. Moorhead, "Operation and Reform of the Classification System in the United States," in *Secrecy and Foreign Policy*, 90. At the time of his writing, Representative Moorhead was Chairman of the Foreign Operations and Government Information Subcommittee of the House Government Operations Committee.

[12] General Accounting Office, *Classified Information: Costs of Protection Are Integrated With Other Security Costs*, NSIAD-94-55 (Washington, D.C.: Government Printing Office, October 1993), 1; Joint Security Commission, *Redefining Security* (Washington, D.C.: 28 February 1994), 115.

[13] Harold C. Relyea, "National Security and Information," *Government Information Quarterly* 4, no. 1 (1987), 11, 19.

[14] Arnold Wolfers, "'National Security' As An Ambiguous Symbol," *Political Science Quarterly* 67 (December 1952), 481-502, cited in Relyea, "National Security and Information," 12.

[15] Commission staff visit to National Security Agency and review of approximately 100 classified documents, 11 September 1996.

[16] Richard M. Neustadt, letter to Chairman Glenn English, 5 May 1982 (House Committee on Government Operations, *Executive Order on Security Classification: Hearings Before a Subcommittee of the Committee on Government Operations*, 97th Cong., 2d sess., 10 March 1982 and 5 May 1982, Appendix 5).

[17] *Department of the Navy v. Egan*, 384 U.S. 518, 527 (1988).

[18] *Youngstown Sheet and Tube Company v. Sawyer*, 343 U.S. 579, 637 (1952).