Summary of Findings and Recommendations

It is time for a new way of thinking about secrecy.

Secrecy is a form of government regulation. Americans are familiar with the tendency to over-regulate in other areas. What is different with secrecy is that the public cannot know the extent or the content of the regulation.

Excessive secrecy has significant consequences for the national interest when, as a result, policymakers are not fully informed, government is not held accountable for its actions, and the public cannot engage in informed debate. This remains a dangerous world; some secrecy is vital to save lives, bring miscreants to justice, protect national security, and engage in effective diplomacy. Yet as Justice Potter Stewart noted in his opinion in the Pentagon Papers case, when everything is secret, nothing is secret. Even as billions of dollars are spent each year on government secrecy, the classification and personnel security systems have not always succeeded at their core task of protecting those secrets most critical to the national security. The classification system, for example, is used too often to deny the public an understanding of the policymaking process, rather than for the necessary protection of intelligence activities and other highly sensitive matters.

The classification and personnel security systems are no longer trusted by many inside and outside the Government. It is now almost routine for American officials of unquestioned loyalty to reveal classified information as part of ongoing policy disputes—with one camp "leaking" information in support of a particular view, or to the detriment of another—or in support of settled administration policy. In the process, this degrades public service by giving a huge advantage to the least scrupulous players.

The best way to ensure that secrecy is respected, and that the most important secrets *remain* secret, is for secrecy to be returned to its limited but necessary role. Secrets can be protected more effectively if secrecy is reduced overall.

Benefits can flow from moving information that no longer needs protection out of the classification system and, in appropriate cases, from not classifying at all. We live in an information-rich society, one in which more than ever before open sources—rather than covert means of collection—can provide the information necessary to permit well-informed decisions. Too often, our secrecy system proceeds as if this information revolution has not happened, imposing costs by compartmentalizing information and limiting access.

Greater openness permits more public understanding of the Government's actions and also makes it more possible for the Government to respond to criticism and justify those actions. It makes free exchange of scientific information possible and encourages discoveries that foster economic growth. In addition, by allowing for a fuller understanding of the past, it provides opportunities to learn lessons from what has gone before—making it easier to resolve issues concerning the Government's past actions and helping prepare for the future.

This does not mean that we believe the public should be privy to all government information. Certain types of information—for example, the identity of sources whose exposure would jeopardize human life, signals or imagery intelligence the loss of which would profoundly hinder the capability to collect critical data, or information that could aid terrorists—must be assiduously protected. There must be zero tolerance for permitting such information to be released through unauthorized means, including through deliberate or inadvertent leaks. But when the business of government requires secrecy, it should be employed in a manner that takes risks into account and attempts to control costs.

It is time to reexamine the long-standing tension between secrecy and openness, and develop a new way of thinking about government secrecy as we move into the next century. It is to that end that we direct our recommendations.

Ours is the first analysis authorized by statute of the workings of secrecy in the United States Government in 40 years, and only the second ever. We started our work with the knowledge that many commissions and reports on government secrecy have preceded us, with little impact on the problems we still see and on the new ones we have found.

In undertaking our mission to look at government secrecy, we have observed when the secrecy system works well, and when it does not. We have looked at the consequences of the lack of adequate protection. We have sought to diagnose the current system, and to identify what works and ways the system can work better. Above all, we have sought to understand how best to achieve both better protection and greater openness.

That the secrecy system that evolved and grew over the course of the 20th century would remain essentially unchanged and unexamined by the public was predictable. It is to be expected of a regulatory system essentially hidden from view. Some two million Federal officials, civil and military, and another one million persons in industry, have the ability to classify information. Categories of administrative markings also have proliferated over time, and the secrecy system has become ever more complex. The system will perpetuate itself absent outside intervention, and in doing so maintain not only its many positive features, but also those elements that are detrimental to both our democracy and our security.

It is time for legislation. There needs to be some check on the unrestrained discretion to create secrets. There needs to be an effective mode of declassification.

To improve the functioning of the secrecy system and the implementation of established rules, we recommend a statute that sets forth the principles for what may be declared secret.

Apart from aspects of nuclear energy subject to the Atomic Energy Act, secrets in the Federal Government are whatever anyone with a stamp decides to stamp secret. There is no statutory base and never has been; classification and declassification have been governed for nearly five decades by a series of executive orders, but none has created a stable and reliable system that ensures we protect well what needs protecting but nothing more. What has been consistently lacking is the discipline of a legal framework to clearly define and enforce the proper uses of secrecy. Such a system inevitably degrades.

We therefore propose the following as the framework for a statute that establishes the principles on which classification and declassification should be based:

> 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.

A statute will not change the current state of affairs overnight, but it will give officials grounds for saying No—and supervisors grounds for asking Why. Secrecy exists to protect national security, not government officials and agencies. There is not the least reason to think that our Government cannot make and then enforce this distinction.

* 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.

A more stable foundation 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, is required. The tendency of individuals in a government agency to protect too much by erring on the side of secrecy will not change through mere exhortation, but only as a result of common principles that are grounded in statutory language. In short, a legislative basis for the classification system, establishing clear guiding principles while retaining broad authority within the Executive Branch to establish and administer the details of the system, offers a better and more predictable way to achieve meaningful changes.

To enhance the understanding of classification and declassification decisions, we suggest adopting the concept of a life cycle for secrets.

All information, classified and unclassified alike, has a life span in which decisions must be made with respect to its creation, management, and use. But the management of classified material should also involve the important consideration of whether the information should be classified at all, and if so, for how long. Some information needs to be kept secret for a day; some for a year; some for a generation or more.

Thinking about even highly sensitive information in terms of its life cycle can help resolve the inconsistencies between the protection that different information requires and the protection it actually receives during different points in its life cycle. The current classification system, however, is notable for the absence of clear standards to gauge the need for and type of protection.

Meanwhile, declassification procedures at the end of the life cycle often fail to distinguish between information that is still sensitive and that which no longer is—resulting in unnecessary protection. The public does have a right to know. A fair amount of information is eventually declassified, but too often—despite some recent examples of successful declassification of large sets of historical documents—only after years of expensive processing (and sometimes lawsuits) under the Freedom of Information Act. The costs of doing business this way are high: in 1992 (the last year for which such data are available), over $108 million dollars was spent simply to process FOIA requests, many of which yielded little or no material that actually was released.

This is hugely inefficient, but at the same time predictable. Government agencies will always feel (and probably *should* always feel) that they have better things to do than worry about and devote resources to declassifying information that may be a half-century old. There are few incentives for agencies to declassify, little accountability of the ways in which they do provide access, and a lack of coherent procedures to gain the release of what no longer requires protection. On the other hand, archivists and historians think there is nothing *more* interesting. And they are not wrong: understanding our past is absolutely crucial to negotiating our future.

To improve declassification procedures, we recommend establishing a national declassification center to coordinate how information that no longer needs to be secret will be made available to the public; among its roles would be to declassify information using guidance from the agencies that originate the information.

Declassification should be seen as a form of deregulation. Currently, there are over 1.5 billion pages of government records over 25 years old in government vaults that are unavailable to the public because they are still classified. Some of these are still highly sensitive and should remain

secret, but others are at the end of their life cycle and should be moved out of the classification system.

The present regulatory system simply will not let go; it will not and cannot declassify enough material in a cost-effective way. The backlog of decades-old classified records exists in part because of the way the Federal Government is organized to provide access. Some systematic mode of deregulation needs to be established: declassification should not be a random procedure. However, because few agencies view this as a primary mission to which resources and expertise should be devoted, timely and cost-effective declassification of older government records of permanent historical value does not now occur.

Central coordination of declassification across the Government, taking into account the fact that the resources available for that activity are limited, is the best means to ensure that the current situation will change. Agency practices need to be identified and explored, not in an adversarial mode, but rather one of constructive oversight that coordinates declassification policy across the Government in a cost-effective way. The task should be given to an existing entity that understands, values, and rewards that activity. The entity that best meets this criterion is the National Archives and Records Administration.

The Declassification Center would perform a variety of services to streamline declassification, provide expertise, allocate resources, act as a clearinghouse for and establish pilot projects to develop new technologies to aid access, and avoid duplicative procurement and activities. Another important component of the Center would be an advisory panel to provide regular public input and advice on agency declassification priorities. The Center would not supersede agency control over substantive declassification decisions; indeed, agency heads may choose not to provide the Center with highly sensitive material. Rather, by promoting a partnership with agencies, enhancing cooperation across different agencies, and using agency-supplied guidance as appropriate, the Center would make declassification a more routine, efficient, and cost-effective process.

Investment in a Declassification Center would pay dividends over time in terms of savings in both financial and opportunity costs. At the same time, the Center would help build greater confidence in the Government's ability to distinguish between core secrets and information that may be made available at the end of its life cycle.

To promote greater accountability, we recommend establishing a single, independent Executive Branch office responsible for coordinating classification and declassification practice and enhancing incentives to improve such practice.

Any policy, including on classification and declassification, is only as good as its implementation. Accountability should be a hallmark of a well-functioning secrecy system. Those charged with creating and maintaining government secrets need to do it well, and they need to know that they will be expected to do so.

Unfortunately, the secrecy system has developed into one in which accountability barely exists. Confusion over the proper roles of existing oversight bodies in the Executive Branch, including the Information Security Oversight Office and the Security Policy Board, has hampered the development and oversight of sound classification policies and practices. The absence of adequate oversight across the Executive Branch and by the Congress has resulted in little accountability for

decisions and little incentive to reduce the scope of government secrecy. We therefore recommend improving training and enhancing incentives so that classifying officials will consider more carefully the costs of secrecy and recognize that they will be accountable for their decisions.

The Commission recommends improving Executive Branch mechanisms by identifying a single office—independent of the agencies that classify and able to demand compliance—that would be responsible for coordinating oversight of classification and declassification practice. This office would make recommendations directly to the National Security Council for establishing classification and declassification policies. It also would ensure that classification and declassification are treated primarily as information management issues, not merely as extensions of security policy. The Commission also proposes improved oversight programs within individual agencies by enhancing positive incentives for officials to improve their handling of classified materials.

To ensure that classification is used more efficiently, we recommend improving the initial classification of information by requiring classifying officials to weigh the costs and benefits of secrecy and to consider additional factors in the decision to make or keep something secret.

The initial decision to classify is critical: it is the most important part of the life cycle of secrets, and the place where the entire regulatory process begins. The decision should be made sparingly, and then vigorously enforced.

Classification means that resources will be spent throughout the information's life cycle to protect, distribute, and limit access to it that would not be spent if the information were not classified. Classification means that those who need to use that information in the course of their work have to be investigated and the results of that investigation analyzed to determine whether access should be granted. Classification means that a document may have to be edited to remove certain sensitive details in order for the rest of the information to be more widely shared inside the Government. And classification means that some kind of review has to take place when the document containing that material is considered for declassification.

The initial decision to classify continues to be based solely on damage to the national security—to the exclusion of other important factors. This has implications both for the quality of protection and the reduction of secrecy overall. Given the importance of this decision, it is essential to develop a more thoughtful process for deciding whether information should be classified in the first place. It is imperative that officials weigh the costs and benefits of secrecy and consider additional factors—such as the vulnerability of the information, the threat of damage from its disclosure, the risk of its loss, its value to adversaries, and the cost of protecting it—in the decision to make or keep something secret.

We recommend that the national security question be weighed differently than heretofore. The issue for classifiers is not just to see if particular information can potentially fit within a category of material that is eligible for protection, but to analyze in the first instance whether information requires the protection afforded by the classification system. Absent a more thoughtful process for making initial decisions, we will continue to see classification by rote, without a careful analysis of whether there is a risk from release of the information that requires it to be protected through classification.

Although there has been progress in reducing the number of individuals authorized to create secrets, much information continues to be classified despite the lack of a national security reason to do so. There have been some serious efforts by agencies in recent years to improve classification management practices. The number of classification actions continues to decline—although in 1995 there were still an estimated 3.6 million new actions, just under 400 thousand of which were at the Top Secret level. Improving the means by which the initial classification decision is made can build on the achievements to date and instill a greater sense of confidence that important secrets will be protected and that other information will be more accessible to the public than at present.

To clarify the grounds for classifying intelligence information, we recommend that the Director of Central Intelligence issue a directive concerning the appropriate scope of sources and methods protection as a rationale for secrecy.

Underlying the rationale of "sources and methods" as the reason that information is kept secret is not the content of the information itself, but instead the way it was obtained. Yet the public and historians generally do not care how the information was collected; they want to know how it was used and what decisions it informed. Too often, there is a tendency to use the sources and methods language contained in the National Security Act of 1947 to automatically classify virtually anything that is collected by an intelligence agency—including information collected from open sources.

A more thoughtful approach is needed to identify and protect the highly sensitive material that needs protection but not overload the system with information that does not require the expenditure of limited resources to protect it. Clarification through issuance of a directive by the Director of Central Intelligence of the scope of and reasons for sources and methods protection would still ensure that sensitive information stays secret. At the same time, such a directive explaining the appropriate scope of that protection would help prevent the automatic withholding of all information that might relate in any manner, however indirectly, to an intelligence source or method.

To promote the use of personnel security resources in a manner that ensures more effective and efficient protection, we recommend standardizing security clearance procedures and reallocating resources to those parts of the personnel security system that have proven most effective in determining who should or should not have access to classified information.

Too often the personnel security system, used to decide whether an individual should have access to particular classified information, focuses resources on policies and programs that apply the wrong type and degree of protection. Today's personnel security system is still based on fear of subversion from Communist agents. This remains the case even though few people join the Government with the intent to commit espionage and, as experience repeatedly has shown, the main threat today comes from trusted "insiders" who already hold clearances and only later in their careers decide to commit espionage, typically motivated by some combination of personal difficulties and greed.

Currently, most resources are directed to the initial clearance process. This includes requiring investigative activities that provide little benefit in comparison to their cost, such as requiring in every instance interviews with neighbors who may barely know the individual under scrutiny.

Meanwhile, relatively less attention is placed on developing more effective procedures for assessing those who already have held security clearances for a number of years.

The Commission recommends directing resources where they are most likely to be of value in determining who should, and who should not, have access to classified information. This means, for example, that those parts of the process—such as neighborhood investigations— shown, both in studies and through experience, not to yield helpful information should no longer be required as a matter of course in every investigation.

The Commission also believes that in order to use resources more effectively, individuals with current clearances should be able to move from one agency or program that requires a particular level of clearance to another that requires a comparable level without replicating investigative and adjudicative procedures. Acceptance by agencies of security clearances granted by other agencies should become the norm, not simply an abstract goal commonly ignored in practice. This should be limited only by the need to take account of different agencies' divergent approaches to the polygraph. Achieving such "reciprocity" would expedite the clearance process and save precious personnel security resources so they may be applied where they can accomplish the most.

To reduce the redundancies and costs of special access programs, we recommend measures to standardize security practices in such programs.

During the course of the Commission's work, industrial contractors repeatedly expressed their concern with the redundancies and high costs of security practices in special access programs: those programs involving security controls that typically exceed what is normally required for access to classified information.

Special access programs can concern research, development, and acquisition activities; intelligence (including covert action); or military operations. Programs can range from rosters specifying who is to have access to the information to entire facilities being equipped with added physical security measures or elaborate and expensive concealment and operational security plans. Such measures often have been justified as the only way to provide the security necessary to protect information considered especially sensitive.

After examination of the oversight and accountability of these programs, the Commission concludes that despite efforts within the Defense and Intelligence Communities to address these problems, many aspects of the system are still in need of repair. Too often, the additional security costs imposed in these programs do not yield increased security benefits. In particular, the Commission believes that a pressing need remains for greater standardization of security practices in special access programs.

To promote more awareness of the threats to automated information systems, we recommend steps to focus greater attention and promote increased cooperation on means for protecting such systems.

This is an era of extraordinary change not only in information technology, but also in the very way that individuals communicate with each other. Information vital to the security and continued prosperity of the United States resides on a series of increasingly interconnected classified and unclassified systems. Those responsible for the protection of national security information face

new and increasingly difficult challenges presented by the widespread use of computer networks linked by telephone lines, cable, direct broadcast service, and wireless communications, and by the proliferation of personal computers. New and rapidly changing electronic information systems, on which both secret and open information travels and is stored are threatened when their protection is not adequate to ensure the integrity of the content and meaning of that information.

This new environment requires a fundamental rethinking of traditional approaches to safeguarding national security information. Despite some recent efforts, however, there are no standards for protecting and managing automated information systems, nor is there any national forum designed to promote cooperation in this area. A more focused and directed approach to oversight of these issues on the part of both the Executive Branch and the Congress, and a reinvigorated and closer cooperation between government and industry, are key to developing and implementing effective and coordinated computer security measures.

In the future, better ways to disseminate threat information, improve public and government awareness of computer attacks and related incidents, and develop means for audit and intrusion detection all will be important to promoting greater awareness of the vulnerabilities to national information systems. The Commission sees it as vital that steps be taken in the near term to address these and other critical protection problems.

This report should be seen as a call for changes that may require years to accomplish and will not occur simply through new regulations or organizational restructuring. Many of the problems identified in the report developed and grew over generations and will not be fixed overnight. Key to ensuring that real change occurs will be the realization by senior government officials—whether career civil servants or political appointees—that it is in their own self-interest, as well as in the country's interest, to gain control over the secrecy system and, by so doing, to promote more effective protection of the information that should remain secret.

To do this properly will require a reevaluation of both how and why information is made secret and whether, how, and when it can later be made available. It will require individual agencies and departments to reexamine how they work together in a range of areas, from declassifying documents to permitting transfer of security clearances and identifying who can be trusted to have access to secrets. Finally, it will require new concepts of how materials can best be protected and, where appropriate, disseminated in an era rich in both information and new technologies.

The United States has successfully dealt with the dangers of the century now coming to a close. A new century awaits with its own dangers—some of which we can sense coming, some as yet untold. National security will continue to be the first of our national concerns, but we also need to develop methods for the treatment of government information that better serve, not undermine, this objective.

The proposals set forth in this report are intended to ensure both that our security endures and our democracy flourishes. Government secrecy is not an abstraction; it affects us all in ways large and small. These improvements are long overdue, and 1997, eight decades since enactment of the Espionage Act and a half century since the National Security Act, is the time to begin.