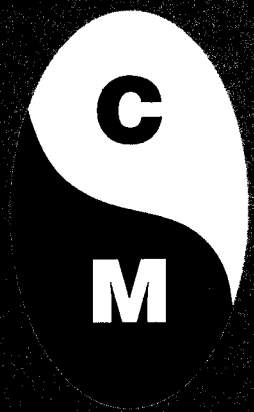
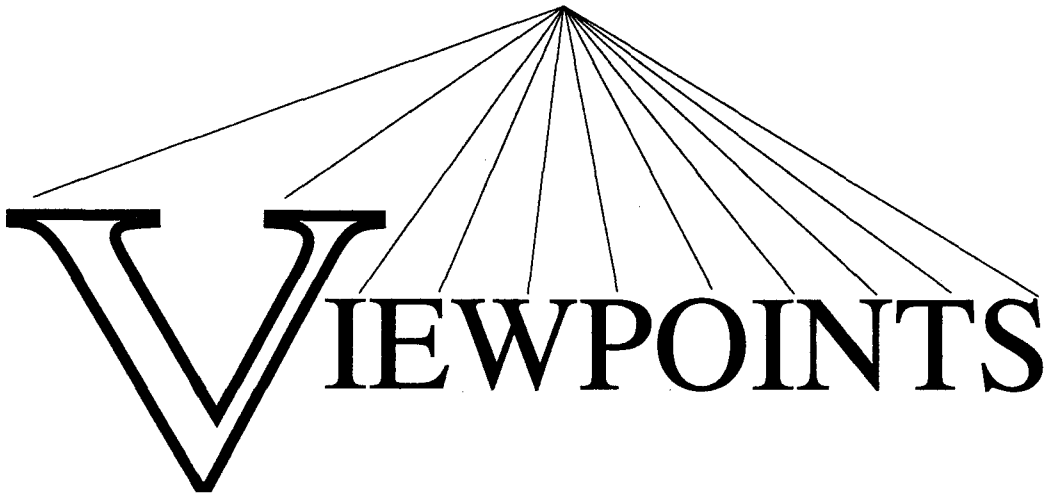


A PUBLICATION OF THE NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME [illegible]

ISSN-0009-8434

Published by the National Classification Management Society. Mailing address: Executive Secretary, NCMS, 2017 Walnut Street, Philadelphia, Pennsylvania 19103. Editor of this -volume: Raymond P. Schmidt. Editorial Review Board: Carol F. Donner, General Research Corporation; Marilyn H. Griffin, Naval Coastal Systems Center; James H. Mathena, Martin Marietta Corporation; Arvin S. Quist, Martin Marietta Energy Systems. Board of Directors Publications Oversight: Dr. Roger Denk, PERSEREC. Publication Coordinator and Publisher: Sharon K. Carter, Executive Secretary. The information contained in this periodical and presented by the several authors does not necessarily represent the views of their organizations or the National Classification Management Society.



PURPOSE

The purposes of the National Classification Management Society are:

- To advance the profession of Security Classification Management.
- To foster the highest qualities of professional excellence among its members.
- To provide a forum for the free exchange of views and information on the methods, practices, and procedures for managing security classification programs and related information security programs.

Members are encouraged to submit articles, think pieces, scholarly studies, and letters about any aspect of classification management and information security. All security subjects are considered for inclusion in ***NCMS VIEWPOINTS.***

PERIODICAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY

TABLE OF CONTENTS

EDITORIAL COMMENTS

Readers will notice several differences in this edition of Viewpoints. Not only is the publication longer, but it also contains several official documents that relate directly to classification management and information security. Beyond those obvious unique aspects, however, is a more fundamental but less conspicuous change. With the first issue of 1995, we welcome the Multiservice Management Company of Philadelphia as our publisher. Ms. Sharon Carter of MMC has taken on the formidable task of converting manuscripts into camera-ready pages of text and illustrations. You are holding the first product of her efforts in your hands.

For this issue, particularly, we express gratitude to the authors who have contributed articles and interviews. They are all among the busiest people in Government and private business, but they willingly took time to share their views with NCMS members. It would be impressive to record the number of hours they devoted to completing articles for our edification. Some of them prepared specific comments in response to questions or a request for a particular piece. Several of the first few were written long before Executive Order 12958 was signed on 17 April 1995, but their content remains fresh and pertinent, as you will see.

This characterization applies to our guest editorial by **Dr. Page Putnam Miller**. Dr. Miller presents the case for creation of a decision-making body of senior agency officials to coordinate the release of information proposed for declassification. She cites problems of overclassification and long delays in reviewing material for declassification. Her article endorses the Interagency Security Classification Appeals Panel created by Section 5.4 of the new Order. One of the Panel's responsibilities will be to facilitate solutions to the enormous tasks of reviewing agency classified information appearing in other agencies' records. If this sounds familiar to readers with security experience dating from the 1970s, you no doubt remember the Interagency Classification Review Committee (ICRC) which carried out these functions. The ICRC was created by President Richard M. Nixon in EO 11652. Its responsibilities were assumed by the Information Security Oversight Office created by President Jimmy Carter in 1978 under EO 12065.

The MITRE Corporation conducted a multi-year study of alternative approaches for automating the declassification review of agency records and for making released documents available to the public via electronic means. Completing the final report in the fall of 1994, MITRE analysts concluded that automation can assist efforts to search for documents, to review and redact them, and to disseminate the declassified product quickly to anyone interested.

Section 3.8 of EO 12958 directs agencies that originate classified information to work with the Director, Information Security Oversight Office to establish a Governmentwide data base of information that has been declassified. The Order also instructs the Archivist of the United States to explore other uses of technology to facilitate the declassification process.

Mr. Howard E. Clark, Mr. Glenn P. Cooley, and Mr. Rex C. Klopfenstein summarize the MITRE report and illustrate the concept of operations. Their 1994 article is still very timely. **Ms. Jacqui Lilly** of the Department of State provided information to prepare a summary of the "FREEDOMS" automated program that has matured and continues to evolve. She emphasizes that one of State's objectives is to be able to provide other interested parties with software to establish similar efforts.

Ms. Ella Nargele and Mr. Ron Benjamin have just declared operational a similar, albeit smaller, effort undertaken by the Navy Historical Center in Washington, DC. They also continue to improve their system, but welcome inquiries from NCMS members who are engaged in declassification review activities.

Executive Order 12951 was signed by the President on 22 February 1995 and is included as an item of interest to members.

Mr. Steven Garfinkel has participated in NCMS meetings for over a decade, and is well known to members. As Director of the Information Security Oversight Office, Mr. Garfinkel has been the focal point (some might say lightning rod) for objections and recommendations to change the current classification management programs. We discussed conducting a virtual interview (in cyberspace) on provisions of the new Order, but neither of us has direct access to the Internet. So the "virtual" interview took the form of an exchange of telefacsimile transmissions. It makes for useful--and entertaining--reading. His office also produced the other information about EO 12958 that is printed in this issue for your benefit. Many NCMS members have a copy of EO 12958, but ***Viewpoints*** advisors urged its publication in whole.

Please note that the effective date of EO 12958 is 16 October 1995, and that five implementing directives must be prepared by the Information Security Oversight Office and the Security Policy Board prior to that date. These will deal with classification and marking, classification and declassification guides, safeguarding, security education and training, and self-inspection programs. Also please note that agency implementing directives and other regulations may provide specific guidance for Government and industry. Consult these before taking action based upon provisions of the new Order.

RAYMOND P. SCHMIDT
June 1995

"Guest Editorial"

Declassification of Historic Records and the Need for an Interagency Review Panel

Page Putnam Miller

In 1993 I became the special investigator for an Organization of American Historians' Department of Defense Legacy grant. The purpose of the grant was to explore the problems that have contributed to the enormous backlog of classified historic records and to prepare four position papers that addressed the most pertinent issues. The papers were written from the perspective of historians seeking to better understand the past but constantly being frustrated by lack of access to crucial policy documents. From the vantage point of historians, the first and major problem contributing to the enormous backlog of classified historical records has been the lack of precise and narrowly defined classification criteria which balances the public's right to know with the protection of sensitive information. The second and third factors are two technical problems-- the handling of "foreign government information" and the decentralization of declassification policy-- both of which have made it difficult for the federal government to release old records in a cost-effective manner. Fourth, we believe that the absence of a high level interagency review panel to coordinate policy and address problems has exacerbated efforts to develop a more workable system.

"The absence of a high level interagency review panel to coordinate policy and address problems has exacerbated efforts to develop a more workable system."

In this article, I wish first to provide some background on why a new declassification policy is important for historians and second to discuss the need for a high level interagency review panel to coordinate policy, a provision which is a part of President William J. Clinton's January 1995 draft of the revision to Executive Order 12356 on classification and declassification policy.

In making a case for increased access to historical documents many decades old, Melvyn Leffler, Chairman of the History Department at the University of Virginia, noted in an address before a Legacy Conference on October 20, 1992, that "A policy of openness breeds understanding of the dilemmas that policy makers faced, of the agonizing decision they had to make, of the excruciating tradeoffs they had to accept, of the incomplete information they had when they could no longer postpone decisions."[1] As Leffler eloquently stated: "Openness leads to understanding, to empathy, to constructive introspection, to healthy criticism. In contrast, a policy of restriction exacerbates public distrust of government which today is omnipresent."[2]

As a consequence of the current classification system, American Foreign and military policy during the Cold War remains poorly understood, not only by the general public but also among scholars and policy makers. Knowledge of the forty years of the Cold War is essential for dealing with the complex relations that are evolving; yet, large gaps remain. The public inaccessibility of historic records from the State Department, the Department of Defense, and other agencies relating to foreign policy has been largely responsible for this situation. Until the last few decades historians were generally able to gain access to historical records over twenty-five years old, but the current system has made it difficult for historians to obtain the primary documents on which to base an evaluation of the policies of the 1950s, 60s, and 70s. In 1994, for example, 1,092 cubic feet of records of the Office of the Secretary of Defense and 805 cubic feet of records of the Joint Chiefs of Staff, all over thirty years old, remained classified. Lack of access to these documents prevents historians from constructing a balanced interpretation of the past and from pointing out the importance of previous experience for understanding contemporary problems.

"A policy of openness breeds understanding[,]...empathy[,]...constructive introspection [, and]...healthy criticism....

"Knowledge of the forty years of the Cold War is essential for dealing with the complex [foreign] relations that are evolving."

The current security classifications policies also separate policy-makers from the lessons of the present. As Representative Lee H. Hamilton, the Democratic Congressman from Indiana who previously chaired the House Foreign Affairs [renamed International Relations in January 1995] Committee, has written: "When important deci-

sions are made in secret, or when information relevant to policy decisions remains unnecessarily secret, this [public] scrutiny is not possible, and policy failures are more likely."[3]

Although current national security policy rests on the assumption that much information must remain secret because its release would be embarrassing, there is strong evidence that keeping documents secret can also be an embarrassment. In an October 30, 1994, *New York Times* article, Tim Weiner explores in depth an episode in which efforts to keep secret CIA activity in British Guyana in the 1960s proved an embarrassment to the Clinton administration. Although the efforts to destabilize the government of Dr. Cheddi Jagan succeeded in the 1960s, Jagan returned to power as president in 1992 in the country's first democratic election in thirty years. In June, the Clinton administration considered as nominee for Ambassador to Guyana a person who had been involved in the 1960s destabilization efforts. According to Weiner, the administration was "apparently unaware that the prospective nominee had helped to undermine the restored leader." In an interview with Weiner about the nomination, President Jagan said he was flabbergasted and conveyed his unhappiness to the Clinton administration. Furthermore, Jagan noted that "Everybody in Guyana knows what happened, I don't understand why they should be left secret."[4] The insistence by the State Department and the CIA that these documents on Guyana remain classified resulted from a dispute between agency declassifiers and the State Department's Advisory Committee on Historical Diplomatic Documentation. The committee recommended that the Foreign Relations of the United States (FRUS) volume dealing with Guyana in the Kennedy Administration not be published because the omission resulted in a distorted account.

The balance to be struck between the basic requirements of national security and the imperatives of democratic government and official accountability is a difficult one, and historians recognize that there are legitimate national security needs that must receive serious consideration in decisions regarding public access to classified federal records. Some types of information obviously need continued protection, such as the identity of confidential, living human intelligence sources whose lives would be endangered if records pertaining to military plans and cryptologic systems currently in use were declassified. Foreign policy records can be especially sensitive, since they often involve negotiations that occur behind closed doors with expressed understandings of confidentiality. Policy-making officials clearly need a guaranteed period of time during which they can entertain full, free, and uninhibited debate with the assurance of confidentiality. Under our system of government, military officers respond to but do not make national defense policy, yet they are responsible for making contingency plans for potential conflicts across the globe which could be harmful or compromising to foreign policy efforts if disclosed. These legitimate concerns must be weighed against the need of the public to investigate the character of the nation's foreign relations. Twenty-five years of classification, and in most cases a much shorter period, should provide the necessary measure of confidentiality to present negotiators.

"Historians recognize that there are legitimate national security needs that must receive serious consideration in decisions regarding public access to classified federal records....[But these] legitimate concerns must be weighed against the need of the public to investigate the character of the nation's foreign relations."

The task of weighing the need to know with legitimate needs to protect information which, if released, could cause damage to the national security is one that should receive high level attention and coordination. One of the most pressing problems in the current classification/declassification system is the lack of coordination between federal agencies in making decisions about what government information is properly classified and what may be publicly released. Formal responsibility for overseeing agency compliance with the executive order on national security information policy rests with the Information Security Oversight Office (ISOO), which has a relatively small staff and reports to the National Security Council (NSC).[5] Although ISOO provides minimal direction through the issuance of regulations and annual reports, each agency currently gives its own interpretation to Executive Order 12356, the presidential directive on classification and declassification, and the implementing regulations that accompany it. Problems of overclassification and lengthy delays in the declassification process are exacerbated by cumbersome review procedures regarding interagency material--that is, the material of one agency that rests in the files of another agency.*

**This is not U.S. national security information policy. Indeed, Section 1.6(a) of Executive Order 12356 expressly prohibits applying a security classification marking on this basis: "In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security." --Editor*

**"Interagency material" is not limited to documents. Rather, any information classified by agency A may appear in documents or databases of agency B, or agency C, D, and E. It is the responsibility of agency A, as the original classification authority for that information, to decide whether it may be declassified. Such classified information is referred to as agency A's classification equity. --Editor*

With no formal procedures for reaching a consensus on what classified interagency material can be declassified and released, each agency tends to act alone. This article reviews past experiences with interagency review panels and discusses the Clinton proposal in the revision to EO 12356 for enhancing the coordination of a uniform and streamlined declassification policy.

During declassification review, use of the designation "Originating Agency's Determination Required" (OADR)--in place of a specific declassification date or event in original classification decisions--increased significantly during the last decade. The General Accounting Office estimated in 1992 that ninety-five percent of all records classified that year bore the stamp of OADR.[6] Similarly, "equity" agreements between agencies that frequently exchange information dramatically extended agency authority over material which it did not create or possess but in which it had some interest. Such a patchwork of policies and authorities has increased costs, caused delays, and frustrated access to historically valuable information. For example, if a memorandum from the Office of the Secretary of Defense is in a Department of State file, the declassification of that file requires permission from the Department of Defense. Because of OADR and "equity" policies,* bulk declassification of older historical material has been impossible.

To help solve these and other related problems, a formal system of interagency coordination is needed. Although precedents for this kind of cooperation do exist, there is currently no such system in place. Consequently, it is common for fifty-year-old records to remain classified because declassification would require dealing with a maze of procedural obstacles. In addition to the intricacies of the review process, there is currently no way to appeal an agency's decision to withhold portions of records from public release, aside from expensive and time-consuming Freedom of Information Act litigation. Under an earlier executive order on classification/declassification, an independent, interagency panel functioned precisely to remedy such problems when they occurred. It is time that a similarly-constituted body be instituted in the reforming of the information security system.

**See the previous explanation of classification equity, which places responsibility for classifying and declassifying a specific element of information on the official who has the formal designation as the original classification authority for that technology, intelligence, system, program, or subject.--Editor*

"One of the most pressing problems in the current classification/declassification system is the lack of coordination between federal agencies in making decisions about what government information is properly classified and what may be publicly released....[Thus,] it is common for fifty-year-old records to remain classified because declassification would require dealing with a maze of procedural obstacles."

The most successful example of an interagency panel charged with brokering classification and declassification disagreements among agencies was the Interagency Classification Review Committee (ICRC) established by President Richard M. Nixon in 1972 as part of Executive Order 11652. Activities of this committee, which met regularly between 1972 and 1978, illustrate that interagency coordination can help develop and apply declassification policy that is responsive to the needs of agencies, scholars, and the general public. Executive Order 11652 created a "continuing monitoring process" under the National Security Council and the ICRC.[7] The order gave the NSC ultimate authority over the security classification system and created the ICRC to "assist" in this task. The order mandated that the Committee "meet regularly and on a continuing basis" and "review and take action to ensure compliance" with the order. Specifically, EO 11652 directed the panel to "oversee Department actions to ensure compliance" with the directive, and empowered the committee to "take action on suggestions and complaints...with respect to the administration" of the order and "assure that appropriate action is taken on such suggestions and complaints".[8] Thus, Committee responsibilities included both monitoring of compliance by various federal departments with the standards of the executive order and review of the overall functioning of the system so that any shortcomings could be detected and addressed.

"Interagency coordination can help develop and apply declassification policy that is responsive to the needs of agencies, scholars, and the general public."

Effective oversight and cooperation was built into the committee by its composition of high-level representatives from each of the federal departments responsible for the majority of national security classification actions. Agencies involved included the State Department, the Department of Defense, the Department of Justice, the Atomic Energy Commission, the Central Intelligence Agency, and the National Security Council. A chairman appointed by the President oversaw the functioning of the committee.[9]

The unique position of the Interagency Classification Review Committee as a coordinating panel with

enforcement powers allowed it to play a significant coordinating role. Perhaps the most fundamental function of the committee was that of fine-tuning the implementation of Executive Order 11652, particularly on issues of declassification. In this respect, the committee interpreted the declassification policies set forth in the executive order for federal agencies and the general public. It also acted as a clearinghouse for suggestions on the improvement of the declassification system. In carrying out these tasks, the ICRC consistently stressed its commitment to openness.

The first chairman of the committee was John S.D. Eisenhower, the son of the former President and a retired Army officer. Eisenhower's appointment gave the committee heightened visibility as well as increased clout. In committee meetings when an agency representative resisted positions advocated by the majority, Eisenhower was known to say to that person something to the effect that "if you continue to adhere to this position, I will have to stop by and talk to Dick about this."[10] The chairman having direct access to the President definitely gave the committee more influence than it would otherwise have had. Although Eisenhower served as chairman of the ICRC for only one year, he established a tone and procedures that were continued by the U.S. Archivist James B. Rhoads, who served as Acting Chairman after Eisenhower's departure.

An example of ICRC's influence is the manner in which it handled the issue of fees. On several occasions agencies wanted to levy fees to offset the cost of searching for, reviewing, and copying classified documents. The regular meetings of the ICRC and high level agency representatives facilitated work toward a consensus on setting fees that did not impede the declassification and release of information. This was accomplished because the committee provided a forum in which to discuss the particular perspectives of the agencies and the legal issues involved.[11]

As required by its mandate under the executive order, the committee continued to strive for genuine openness on other information security issues. At a meeting in May 1973, the panel discussed agency authority to exempt large amounts of information from the General Declassification Schedule established by Executive Order 11652. James B. Rhoads, who became acting chairman of the ICRC in 1973 and continued in that position until the committee was disbanded, set the tone of this meeting by stating at the outset that "our objective is to devise a system or evolve our present system in a way that is conducive to the minimal exercise of exemption authority." After input from the various agency representatives on the particulars of exempting documents from automatic declassification, the chairman appointed a working group to study the use of exemption authority and "to make recommendations on the most effective way of keeping to a minimum the amount of material exempted from the General Declassification Schedule." The goal of the working group was a recommendation to the President on amending the executive order itself to close this potential loophole.[12]

On another occasion standard ICRC oversight procedures resulted in a change in the implementing regulations for the executive order. In a regular survey of agency statistics on implementation, the committee noticed a surge in instances of "classification abuses." The committee discussed at length the matter of "abuses" and the ramifications for both the "abuser" who was subject to reprimand and the extent of disclosure. After input from all sides, the panel concluded that a vague definition of "classification abuses" was largely responsible for the rise in "abuses." The members voted to distinguish in the implementing regulations between unnecessary classification and intentional overclassification.[13]

Another task of the Interagency Classification Review Committee central to its coordination and oversight of declassification policy was its service as an appeals panel. The Committee heard and decided appeals when an originating federal agency refused a researcher's request to declassify certain documents. The ICRC assumed this function on the basis of specific language in Executive Order 11652. As noted earlier, the order gave the Committee's parent agency, the NSC, overall authority for implementing the order but also gave the Committee itself authority to "take action on suggestions and complaints from persons within and without the government with respect to the administration" of the order.[14]

On several occasions the ICRC used its authority as an appeals panel to reverse agency withholding decisions. At its January 1973 meeting, for instance, the committee considered the request of a researcher for the declassification of several Joint Chiefs of Staff documents from 1950. Although the Atomic Energy Commission representative pointed out that he "did not foresee any appreciable negative impact" from the release of the twenty-two-year-old documents, both the NSC and the Department of Defense representatives opposed releasing the information on the grounds that such action could damage current foreign relations. Despite such objections from the originating agencies, the panel voted to declassify the documents. At the same session, the committee overruled an NSC withholding decision, with the NSC representative casting the lone vote for continued classification.[15]

"An appeals mechanism therefore increased accountability within the information security system by requiring substantive justification for continued classification."

When the committee voted to uphold an agency's decision to continue classification, it made sure it was thoroughly informed as to the reasons for continuing classification. On one occasion, an additional representative of the Central Intelligence Agency appeared at the ICRC meeting to present sanitized versions of requested CIA material that was then on appeal. Although the committee eventually voted to release the CIA documents in sanitized form, the representative found himself "questioned closely" on the criteria cited by the CIA for the continued classification of the "deleted portions" of the documents. He was also "asked to give a detailed explanation for the CIA's decision regarding [the] documents and to give an estimate of the impact that disclosure of [the] material could have on national security."[16] Such an appeals mechanism therefore increased accountability within the information security system by requiring substantive justification for continued classification.

During its lifespan the ICRC facilitated declassification with other steps that could have been taken only by an interagency group. For example, the committee oversaw a "government initiated" project in which the Department of Defense, the State Department, and the CIA worked together to collect and sort, for declassification and release, historical records on particular post-World War II international crises.[17] Similarly, in its first years the ICRC formed a Computer Working Group to coordinate implementation of a government-wide data index for classified material. The index was to "provide a tool for the agencies and the ICRC to monitor the classification of documents and to ensure that such material is being declassified at the earliest possible time." The data index, as a systematic means of tracking classified information in a uniform manner throughout the federal government, never emerged in workable form. Several agencies cited the prohibitive costs involved as grounds for their opposition.[18] The point here, however, is not to advocate a database as a tool for declassification, but to note that the ICRC provided a mechanism for formal coordination. Its success was all the more impressive given the fact that it never had adequate institutional support, staff, or resources to pursue the significant responsibilities with which it was charged under the order.[19]

"ISOO...[used] its small staff and modest resources almost solely to report classification statistics, to prepare an annual report, and to conduct occasional on-site inspections at specific agencies."

This vital activity terminated under the administrations of Presidents Jimmy Carter and Ronald Reagan. Beginning in 1978 with President Carter's Executive Order 12065, the general oversight and reporting functions of the ICRC were transferred to the director of the newly created Information Security Oversight Office (ISOO).[20] ISOO soon began to use its small staff and modest resources almost solely to report classification statistics, to prepare an annual report, and to conduct occasional on-site inspections at specific agencies.

As part of the shifting of function, the Carter order directed ISOO to "consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program, including appeals from decisions on declassification requests."[21] There was little time available, however, to consider and implement suggestions. The Carter order also established an **"Interagency Information Security Committee,"** composed of representatives from the same agencies that had representation on the ICRC, with the addition of the Treasury Department. However, the committee had no authority and was not required to meet regularly. The order's language only directed that the panel advise the chairman, who was the ISOO Director, on implementation of the order.[22]

These kinds of changes escalated after President Reagan issued Executive Order 12356, which went into effect on August 1, 1982. The Reagan order eliminated both the interagency advisory panel and the language that had given the ISOO Director authority to hear appeals on declassification requests.[23]

The Clinton administration's January 1995 draft executive order on national security information attempts to restore the kind of formal mechanism for interagency cooperation and declassification oversight that had been eliminated under the Carter and Reagan orders. The draft proposed executive order would create an **"Interagency Security Classification Appeals Panel."** As its name indicates, the panel would be responsible for returning to the classification/declassification system some of the most useful functions of the old ICRC, namely, hearing and deciding on "appeals by persons who have filed declassification challenges" and approving, denying, or amending agency exemptions from automatic declassification. The panel would be given direct authority to act as a high-level arbiter of declassification decisions.[24]

In addition to creating the **Interagency Security Classification Appeals Panel**, the Clinton 1995 draft

order would establish an **"Information Security Policy Advisory Council,"** a body of non-governmental "interested persons" that would perform in an advisory capacity some of the independent oversight functions formerly administered by the ICRC. In particular, the Council would advise the President, the NSC, and ISOO on the policies established by the executive order, "including recommended changes to those policies." The Council would also work with individual agencies to prioritize records that need to be declassified and provide a public forum for discussion of controversial issues in federal government information policy.[25]

Although the two most recent executive orders on national security information did not mandate such a formal interagency panel, other means of facilitating interagency cooperation for declassification have evolved. Problems that had arisen in the compilation of the century-old Foreign Relations of the United States (FRUS) series provide a prime example of the need for formal interagency cooperation in declassification. Attempted resolutions of some of the issues involved in this particular endeavor have gone far to build interagency cooperation into the information security system.

"Problems...in the compilation of the century-old Foreign Relations of the United States (FRUS) series provide a prime example of the need for formal interagency cooperation in declassification."

In 1990 the State Department conducted an in-house review of the FRUS publication process after the integrity of the series was called into question because of deletion of information and the inaccuracies that arose from these omissions. The study found that department historians and members of the Department's **Advisory Committee on Historical Diplomatic Documentation**, all with the necessary security clearances, often did not have adequate access to evidence documenting foreign policy formulation that was held by agencies other than the State Department. The study noted that expanded access to other government agencies "is central to an accurate and comprehensive documentary record."[26] The State Department Reauthorization Act for 1992-93, therefore, attempted to address this problem by mandating that any arm of government involved in the formation of foreign policy must "cooperate with the Office of the Historian by providing full and complete access to the records pertinent to United States foreign policy decisions and actions" and develop procedures "to coordinate with the State Department's Office of the Historian in selecting records for possible inclusion in the FRUS series."[27]

Specifically, the Reauthorization Act required such agencies to allow "full access to the original, unrevised records by such individuals holding appropriate security clearances as have been designated by the Historian as liaison" to that agency, including members of the Advisory Committee on Historical Diplomatic Documentation. Under the Act, each agency retained its own procedures for declassification review, but was compelled to provide timely, written justification to the State Department for any exemptions from the FRUS series that it may eventually require. The Act also gave both the State Department Historian and the Advisory Committee limited powers to reach an agreement with an agency on disclosure if either party determined that such exemptions would cause the FRUS volume to present "an inaccurate or incomplete historical record."[28]

Unfortunately, the integrity of the FRUS series is not guaranteed because the goal of full interagency cooperation remains unfulfilled. Despite enactment of the 1992-93 reauthorization legislation, the agencies outside the State Department that are most involved in formulating foreign policy have not yet fully cooperated with Historian's Office and the Advisory Committee. Too often the deadlines stipulated in the legislation have gone unheeded. In its 1992 report to the Secretary of State, the Department's Advisory Committee cited "delays in declassification reviews by other agencies or governments" as one of the primary problems hampering its work.[29] Not surprisingly, the committee also remarked to the team working on the Clinton draft order that its own experience "demonstrates the unquestioned necessity for a body with full authority and responsibility to monitor" the classification/declassification system.[30]

The most recent attempt to facilitate interagency cooperation on declassification also appeared in the form of legislation. Public Law 102-525, signed by President Bush in October 1992, established an **"Assassination Records Review Board"** to oversee the public release of all government records relating to the assassination of President John F. Kennedy. According to the law, the primary duty of this panel of non-governmental scholars and professionals is to "consider and render decisions on a determination by a Government office to seek to postpone the disclosure of assassination records."[31] In practical terms, the board is to serve as a check on government agencies which are reluctant to declassify and disclose those assassination-related records in their possession which are no longer sensitive for national security reasons. To carry out this task, the law gives the Review Board significant power, including the authority to "direct Government offices to transmit to the Archivist assassination records as required" under the Act and to "obtain access to assassination records that have been identified and organized by a Government office." The President has the sole authority to overrule

a decision of the Review Board regarding disclosure of a particular assassination record.[32] Although the legislation became law in the fall of 1992, the Review Board members were not confirmed until the spring of 1994. Due to the delays in the nomination process, the Board did not become functional until late 1994; however, its independence and government-wide authority could serve as a model for interagency oversight of a revised classification/declassification system.

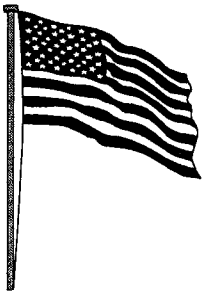
"Formal coordination among government agencies is required to reform the information security system."

Formal coordination among government agencies is required to reform the information security system. In the past, declassification policies in different agencies have conflicted with one another. This not only wastes time and resources, but also constrains access to information that is needed to understand the past and chart the future. Centralization in the process of interpreting and implementing a new executive order would streamline the entire system. This could be accomplished by an interagency panel with sufficient authority, staffing, and resources. The Clinton January 1995 draft Order moves in this direction by setting up an appeals panel that presumably would apply standardized criteria to contested declassification decisions. The draft Order also would create a non-governmental council to help oversee the entire information security system. It is time for such cooperation among different branches of government and the wider public to replace the current patchwork of authorities, policies, and interpretations that has heretofore guided the system.

Dr. Page Putnam Miller is Director of the National Coordinating Committee for the Promotion of History and a regular contributor of Perspectives, a monthly (less July-August) newsletter of the American Historical Association. She remains current on executive and legislative actions that affect public access to official information, and reports on legal proceedings regarding these actions.

Footnotes

1. Melvyn Leffler, "Writing Postwar National Security History: A Plea for Cooperation," unpublished paper presented on October 20, 1992, at a Department of Defense, National Archives and Records Administration Declassification conference, p.6.
2. Ibid. p.20.
3. Lee H. Hamilton, "The Costs Of Too Much Secrecy, *Washington Post*, April 13, 1992.
4. Tim Weiner, "A Kennedy-CIA Plot Returns to Haunt Clinton," *New York Times*, October 30, 1964.
5. Executive Order 12356, Sec. 5.2.
6. United States General Accounting Office, "Classified Information: Volume Could Be Reduced by Changing Retention Policy," (May 1993), pp.16-17.
7. Harold C. Relyea, Congressional Research Service, "The Evolution of Government Information Security Classification Policy: A Brief Overview (1972-1992)." 1992.
8. Executive Order 11652, "Classification and Declassification of National Security Information and Material," (March 8, 1972), Section 7(A).
9. Executive Order 11652, Sec. 7(A). Another Executive Order in 1973 appropriately added the chief records manager in the federal government, the Archivist of the United States, to the committee's membership.
10. Conversation between Page Putnam Miller and James B. Rhoads, who succeeded John Eisenhower as Chairman of the Interagency Classification Review Committee (ICRC), in September 1994.
11. Minutes, Meeting of the ICRC, August 21, 1974, pp.6-7; November 20, 1974.
12. Ibid., April 23, 1973, pp.5-6.
13. Ibid., September 26, 1976, pp.3-4; October 27, 1976, pp.3-4.
14. Executive Order 11652, Sec. 7(A).
15. ICRC Minutes, January 10, 1973, pp.3-4.
16. Ibid., March 24, 1976, p.2.
17. Ibid., June 5, 1972, p.7.
18. Ibid., December 6, 1972, pp.1-2; November 7, 1973, p.4.
19. Relyea, pp.11-12.
20. Executive Order 12065, "National Security Information," (June 28, 1978), Sec. 5-2.
21. Ibid., Sec. 5-202(b).
22. Ibid., Sec. 5-3.
23. Executive Order 12356, "National Security Information," (April 2, 1982), Sec. 5.2 generally; 5.2(b)(6).
24. Draft Clinton Executive Order, "National Security Classified Information," (January 1995), Sec. 5.4.
25. Ibid., Sec. 5.5.
26. William Slany, "Status of the Foreign Relations Series: A Report," November 1990, p.3.
27. 22 U.S.C., Sec. 4352-3, 1991.
28. Ibid., Sec. 4353.
29. State Department Historical Advisory Committee Report, November 10, 1993, p.3.
30. Ibid.
31. 44 U.S.C., Sec. 2107, 1992.
32. Ibid.



Executive Order 12951 of February 22, 1995

Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to release certain scientifically or environmentally useful imagery acquired by space-based national intelligence reconnaissance systems, consistent with the national security it is hereby ordered as follows:

Section 1. *Public Release of Historical Intelligence Imagery.* Imagery acquired by the space-based national intelligence reconnaissance systems known as the Corona, Argon, and Lanyard missions shall, within 18 months of the date of this order, be declassified and transferred to the National Archives and Records Administration with a copy sent to the United States Geological Survey of the Department of the Interior consistent with procedures approved by the Director of Central Intelligence and the Archivist of the United States. Upon transfer, such imagery shall be deemed declassified and shall be made available to the public.

Section 2. *Review for Future Public Release of Intelligence Imagery.* **(a)** All information that meets the criteria in section 2(b) of this order shall be kept secret in the interests of national defense and foreign policy until deemed otherwise by the Director of Central Intelligence. In consultation with the Secretaries of State and Defense, the Director of Central Intelligence shall establish a comprehensive program for the periodic review of imagery from systems other than the Corona, Argon, and Lanyard missions, with the objective of making available to the public as much imagery as possible consistent with the interests of national defense and foreign policy. For imagery from obsolete broad-area film-return systems other than Corona, Argon, and Lanyard missions, this review shall be completed within 5 years of the date of this order. Review of imagery from any other system that the Director of Central Intelligence deems to be obsolete shall be accomplished according to a timetable established by the Director of Central Intelligence. The Director of Central Intelligence shall report annually to the President on the implementation of this order.
(b) The criteria referred to in section 2 (a) of this order consist of the following: imagery acquired by a space-based national intelligence reconnaissance system other than the Corona, Argon, and Lanyard missions.

Section 3. *General Provisions.* **(a)** This order prescribes a comprehensive and exclusive system for the public release of imagery acquired by space-based national intelligence reconnaissance systems. This order is the exclusive Executive Order governing the public release of imagery for purposes of section 552(b)(1) of the Freedom of Information Act.
(b) Nothing contained in this order shall create any right or benefit, substantive or procedural, enforceable by any party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

Section 4. *Definition.* As used herein, "imagery" means the product acquired by space-based national intelligence reconnaissance systems that provides a likeness or representation of any natural or man-made feature or related objective or activities and satellite positional data acquired at the same time the likeness or representation was acquired.

WILLIAM J. CLINTON
February 22, 1995

The Need for an Interagency Declassification Support System

Howard E. Clark
Glenn P. Cooley
Rex C. Klopfenstein

Background and Scope of Article

This article is based on a recent MITRE Corporation study that was sponsored by two federal agencies: the National Archives and Records Administration (NARA) and the Information Security Oversight Office (ISOO). The purpose of the study was to analyze how automation could benefit the declassification efforts of the federal government. The study developed requirements and costs for an automated system (called the Interagency Declassification Support System, or IDSS) that would facilitate individual agencies' declassification activities and provide an interagency database of declassified documents that are released to the public. The interagency database would enable agencies to coordinate their declassification efforts. A key feature of the IDSS is that it would be an integrated system, but the database would be distributed so that each agency could manage its own portion. For public access, each agency could make a copy of its portion available via the Internet.

Cost estimates were made to aid agencies in costing the implementation of the IDSS within their own organizations. The cost estimates were based on ranges of the number of pages reviewed annually in declassification activities, and were developed in sufficient detail to apply to various modular implementations of the IDSS. To derive a cost estimate for its own operations at a particular location, an agency would use its estimate of annual processing volume and select the components of the IDSS that it wished to implement. The scope of MITRE's cost estimation included interagency operations but not public usage of the database; agencies would need to estimate the cost of this capability separately.

The 17 March 1994 draft version of the new Executive Order on Classified National Security Information assigned NARA (in conjunction with ISOO and other agencies) the responsibility of establishing a government-wide database of declassified information. Assuming that this provision is retained in the final version as ordered by President William J. Clinton, a system such as the IDSS will be required. At present, the IDSS is a conceptual system. Some agencies are proceeding with development of internal systems to aid the processing of information requests and declassification reviews, but development of an integrated, interagency system with IDSS capabilities has not been undertaken.

This article begins with a description of problems associated with the current declassification process and then presents the architecture and concept of operations of the proposed IDSS. Conclusions and recommendations are stated at the end.

Problems With The Current Declassification Process

The Clinton administration wishes to declassify and release to the public as much as possible of the government's holdings of national security classified information. In Fiscal Year (FY) 1993, 6.6 million pages of previously classified documents were declassified and made public (30 percent fewer than in FY 1992). In both FY 1992 and FY 1993, however, classification actions (including original and derivative decisions) exceeded six million. Because most of these actions involved multiple pages, and each is subject to many reproductions, the number of new classified pages produced in these years greatly exceeded the number of pages declassified. Meanwhile, there are many hundreds of millions of older classified pages in government archives, storage, and files.

Classified documents frequently exist in multiple copies, filed in different agencies or in different components of the same agency. Over time, therefore, multiple declassification reviews of the same document may occur. Interagency mechanisms for the exchange of declassification actions on documents (i.e., outcome of the review of a document, such as declassification of a document in its entirety, partial declassification, or denial) presently do not easily or routinely support declassification actions on all copies of the same document.

An agency seeking to review documents containing information originating within the agency can handle the review internally. Often, however, the agency's files include documents that originated in another agency or that contain classified information gained from another agency, necessitating coordination between the agencies. Coordination is time-consuming and labor-intensive for both referring and originating agencies.

Agencies sometimes do not know where all copies of a document reside and thus may be unable to notify all other holders of the document when a declassification decision has been made. Some, but not all, agencies have systems to track previously

declassified documents. The existing tracking systems serve individual agencies. It is quite possible for a single document to be classified in the files of one agency while it is unclassified in another, and, if previously reviewed, declassified in part in a third.

In addition, agencies have difficulty maintaining consistency in handling requests for the same document. In Congressional hearings in 1990, two versions of the same released document were exhibited, where the second version showed more excisions than the one released first. Thus in the second version, the agency was restricting information it had previously made public. MITRE found several examples of this problem in an examination of randomly selected, declassified documents collected by the National Security Archive, a non-government organization of foreign policy analysts.

In addition to document inconsistency and slow referrals, agencies have indicated that their procedures for manual redaction of documents under review can be cumbersome and slow, involving markup, cut-and-paste operations and repeated photocopying. Agencies also point out that the availability of up-to-date declassification guidelines can be a problem, and with many guidelines to access in a declassification review, their use can be slow and tedious.

How Automation Can Help

Short of massive bulk declassification (which is not feasible for some types of documents because their content necessitates line-by-line review), how is the government to expedite the declassification review and referral processes and reduce the occurrences of inconsistency? The solution lies in a more extensive, effective use of computer technologies such as relational databases, document imaging, sophisticated text search and retrieval software, state-of-the-art data storage technologies, case tracking and workflow software, and the use of wide area networks for data communications among and between agencies and the public.*

Well-conceived, coordinated development and use of such technologies can solve some declassification problems in the following ways:

- The availability of a database of declassified documents from multiple agencies can reduce instances where agencies are inconsistent in declassifying the same material. The immediate availability of up-to-date versions of declassified documents of other agencies should increase dialogue between agencies when potential conflicts surface, and prevent inconsistent review results from being released.
- The use of shared, wide area network (WAN) based electronic databases of declassified documents among agencies can increase the overall information available to a reviewer, resulting in higher quality reviews. The availability of a searchable database of declassified documents from other agencies may enable an agency to avoid a referral in cases where they can locate a document at another agency that has already been declassified for the specific information under review.
- The public availability of a searchable database of declassified documents, either over WAN access services or through reading room terminals, would enable public users to view documents directly. When those individuals see the documents (even with redactions), they may determine that the information they are seeking is in the documents and thus a declassification review would not be needed. Also, public users might note when the last review took place, and if recent, might decide that an additional review was unnecessary. Avoiding unnecessary reviews, and avoiding dealing with repeated requests for them, would save agency resources.
- Databases and text-search engines can provide a fast electronic document search capability that would reduce the time that agency support staff and/or reviewers spend in searching for documents relevant to an information request. In addition, the speed at which electronic databases can be searched and information retrieved (as opposed to manual methods) allows for more thorough searches, which could reduce the number of repeat requests.
- High-density storage technologies can allow agencies to store vast quantities of documents electronically on-site, eliminating the need to access physical storage warehouses off-site. Electronic storage, to the extent that it can replace collections of actual hard copy documents, takes much less space than the paper versions.
- An automated redaction capability can greatly reduce the time spent on labor-intensive, manual cut-and-paste redaction operations. Computer automation and imaging technology can provide a quick and efficient means to redact text in screen images of documents and print the declassified version to send to requesters.

**Some agencies have initiatives to increase the application of computer technology in declassification. For example, the CIA is building a classified case tracking/document review system under its MORI (Management of Officially Released Information) project. Other agencies with similar efforts include the FBI and the State Department.*

IDSS ARCHITECTURE

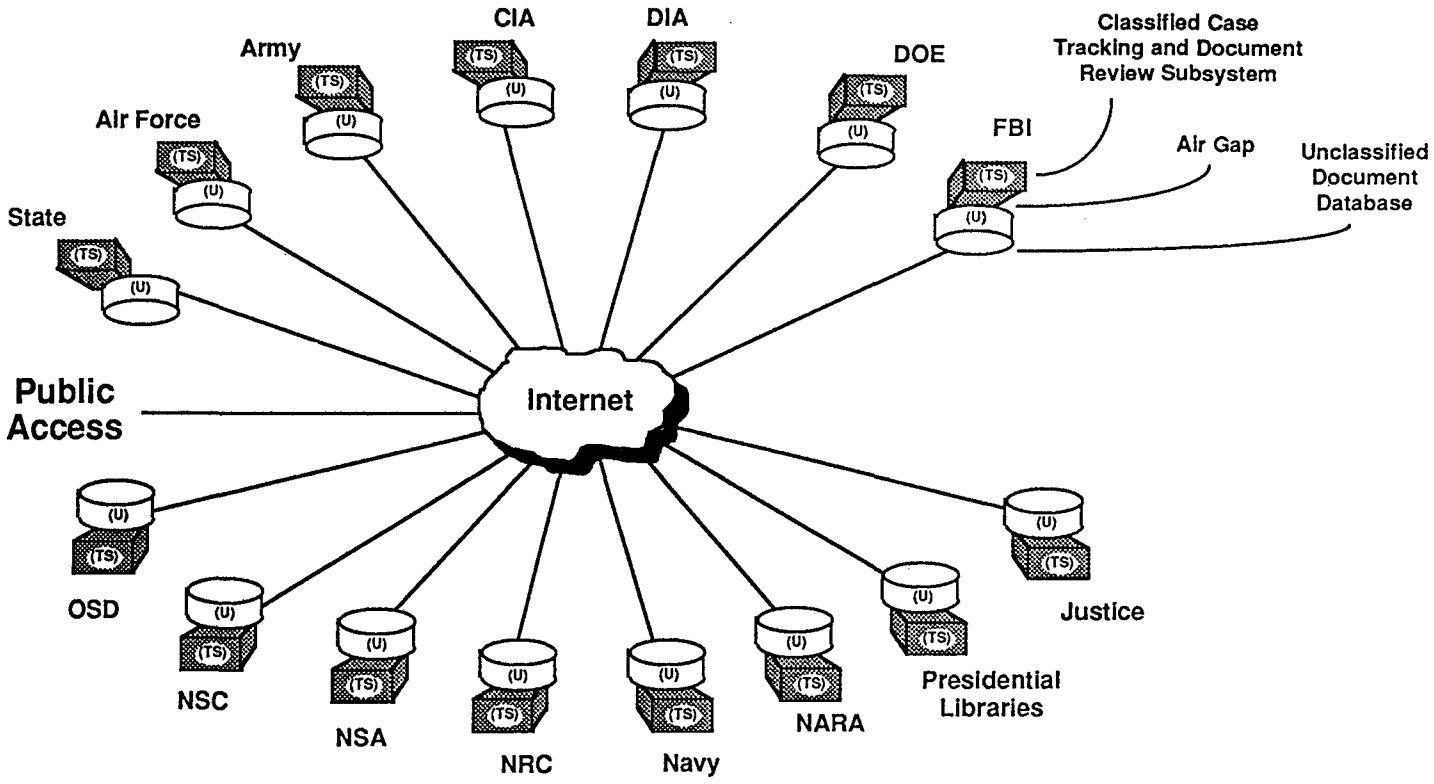


Figure 1

TS = Top Secret
U = Unclassified

- Automation can be used to store the full text of declassification guidelines in electronic databases that are easy to search in a variety of ways and, through a graphical user interface, can show the guidelines on-screen simultaneously with the document being reviewed. Relevant guidelines can be made easier to find and use. They can be kept up-to-date more easily, and distributed instantaneously.

Of course, learning that a requested document has already been declassified and released would avoid having to conduct a declassification review entirely. Many documents do not require any security protection or withholding for any other reason after the initial review.

When taken together, there could be considerable savings in work time through the elimination of tedious labor-intensive tasks such as photocopying, searching files, and redacting documents. The labor savings should enable agencies to process requests more rapidly, thus getting the information to requesters in a shorter period of time. In addition, on-line public access to declassified documents could help to offset the expanding volume of requests for information.

System Architecture

The initial thrust of the study was to determine the feasibility and usefulness of a centralized, unclassified database containing declassified documents from various civilian, defense, and intelligence agencies. Government agencies would have on-line access to this database, as would the public. During the course of the study, the database concept evolved. Discussions with fifteen agencies and a significant increase in the use of the Internet by the government (as well as the public) led to the view that the unclassified database could be distributed across participating agencies. Each agency could maintain its own database. By use of the Internet and its search and discovery software, the collection of agency-maintained databases could be treated logically as a single database. It also became clear that each agency would need a classified component to support its document declassification efforts and to prepare the newly declassified documents for storage in the unclassified database component. Some agencies were already pursuing this goal.

Figure 1 shows the architecture of this Internet-centered view of the proposed IDSS. Note

that the Internet connects only to the unclassified component and that the classified and unclassified components at each agency are not connected. Future technological advances may allow secure, one-way connections between classified and unclassified components of a system, but the proposed IDSS architecture does not assume that such a connection is feasible at this time.

Discussions with agencies indicated the need for a scaleable system. An upper limit appeared to be the reviewing of a million pages per year for declassification at a single location. Other locations might review only 50,000 pages per year. Moreover, some agencies currently do not declassify documents at a single location, but have many locations. Some declassification locations in an agency are temporary, where declassification teams are sent to process a fixed set of documents and then leave when the task is completed.

A key to the proposed IDSS architecture is the use of commercial-off-the-shelf (COTS) software for workflow, page scanning, optical character recognition (OCR), text search, redaction, database management, and Internet access. Modular COTS software is readily available for all of these areas except for redaction. A survey was unable to identify self-contained redaction software packages that could present page images to reviewers and provide the graphical tools needed to obscure and annotate still-classified passages within those pages. Redaction software does exist within proprietary document-imaging software packages, and reusable code is available that could be assembled into a self-contained redaction package, so obtaining redaction software for use in the IDSS should not be overly difficult.

Along with the use of COTS software packages, the IDSS architecture would use standard file formats for plain text, page images, and case tracking data files. Commercial full text software packages use very compact, proprietary formats for their text indexes. The architecture of the IDSS presupposes the use of proprietary file formats for these index files.

Defining standard file formats for exchange of data between software packages helps to achieve the desired scaleability in the proposed IDSS. Moreover, it provides a means of integrating the IDSS with existing declassification software at some agencies and with software that is now under development. At the high end of the IDSS spectrum, where a million pages of classified material are to be processed annually, we envision a classified component consisting of a local area network (LAN) with more than 60 workstations for document search, document review and redaction, workflow control, and system administration. These workstations would access page scanning servers controlling up to three scanners, print servers controlling up to nine printers, full text search servers, and database management servers. The full text search server would access document indexes. The database management server would provide access and storage for page images (the bulk of storage needs), declassification guidelines, and case tracking data. The storage for these two servers could be apportioned over primary and secondary storage devices. These devices would be selected according to speed of access and volume of storage, where the primary storage devices would be faster than the secondary ones and would have less storage capacity. The unclassified component of this high-end IDSS would contain an Internet Wide Area Information Server (WAIS) accessing a database of indexed text and corresponding page images.

At the small end of the IDSS spectrum there would be a desktop unit for classified processing that would have the same IDSS functionality as the high-end system but much less storage capacity. In between would exist systems of varying capacities and functionality. Some agencies stated that they would not need all the functions that were proposed for the complete IDSS. For this reason, the architecture was designed to be modular in function as well as size.

IDSS Concept of Operations

Agencies would use the IDSS to record, track, and acknowledge information requests; to select and review documents related to the request; to declassify or redact some or all of those documents; and to disseminate the declassified or redacted ones by sending them to the requester and making them available to other agencies and the public. When necessary, an agency will use the IDSS to refer documents containing equities* of other agencies to those agencies for review. Likewise, an agency will use the IDSS to respond to referral requests from other agencies.

In the following discussion, we assume a division of labor with different individuals performing different operations. This division, used for the sake of discussion, does not preclude one or a few individuals from performing all operations. In fact, all operations could be consolidated on a

**Classification equities of an agency are those information elements that have been determined to require security protection by an original classification authority of that agency. It may be referred to as that agency's information. --Editor*

DECLASSIFICATION PROCESS WORKFLOW

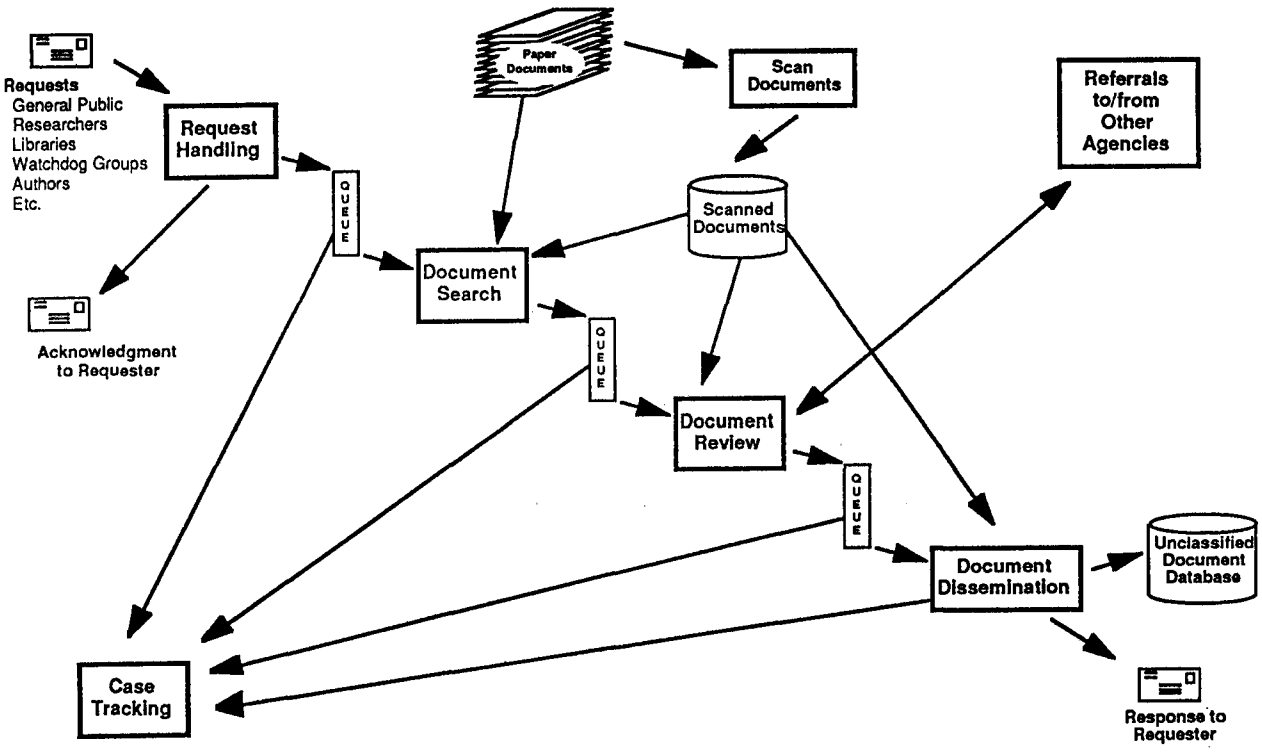


Figure 2

single desktop platform in small declassification offices. We will also discuss operations that would be performed automatically by the IDSS. **Figure 2** shows the main declassification workflow related to the operations discussed in the rest of this section.

It is currently assumed that information requests would arrive at an agency by mail (in the future, electronic requests and submissions are expected). In interviews with agencies, we discovered that they insist upon written requests for tracking purposes and as a means of filtering out non-serious requests. A receiving agent would log the request, scan the pages of the request, and send an acknowledgment to the requester. The IDSS would queue the request for further processing.

After opening the information request letter, a receiving agent would open a new case in the IDSS and complete an electronic form presented by the system. The system would automatically assign a case number when a new case was opened. The form would provide entry boxes for the following minimum set of data: postal cancellation date from the envelope, the current date (automatically supplied), the name(s) of the requester(s) and their address, and the number of pages contained in the request letter. After the receiving agent has completed the electronic form, the IDSS would print an acknowledgment form for mailing to the requester. By law, Freedom of Information Act requests must be acknowledged within ten days. The receiving agent would then mail the acknowledgment.

Once the request had been logged, the receiving agent would either scan the pages of the request into the IDSS or would submit them for scanning by others. Either way, the case number assigned by the system during login and the page count entered by the receiving agent would be used by the system to associate the scanned pages with the case.

After the request was logged as a case and its associated pages scanned, the IDSS would enter the case into a document search queue for the next processing step. Document searchers would respond to requests found on the queue, looking for documents that might be relevant to the specified case. They currently work on a first-in-first-out (FIFO) basis (according to law), although there may be some rare exceptions. The IDSS design assumes this same FIFO basis and therefore provides work queues for the document searchers that contain references to cases as they are received. As relevant documents are found, they would be linked to the case for the next step of document review. After studying the original request, a searcher might look for relevant paper documents in local archives and for electronic versions of documents stored within the IDSS.

The methods and criteria for finding paper documents in local archives will not be addressed here. It is assumed that existing procedures would be followed at first. For each paper document selected for review, the document searcher would associate it with the current case. A document searcher would enter the following data (if available) into the IDSS to identify a document: location of the paper version of the document within the local archive, document owner (originating agency), document name, document number and/or version, author(s), links to other agencies when known, and date of origination or span of dates for multiple version documents. The document searcher might also enter keywords and an abstract if they were available and time permitted. The IDSS would assign a system document number to the document and print a scanner cover sheet that would contain the document number and the case number. The document searcher would place this cover sheet on top of the paper document for later use when the document was scanned.

To look for electronic documents already stored within the IDSS, the document searcher would formulate a set of queries based on words and phrases pertinent to the case and submit them to the IDSS. The system would respond to two kinds of queries: one directed to document catalogs within the IDSS and the other directed to the full-text search servers within the IDSS. The catalogs would contain information about documents, such as keywords, title, and authors. The full-text search servers would have access to document contents through indexes that were built and updated using text obtained by OCR conversion of document page images scanned into the IDSS. Either method would give the document searcher a rank-ordered list of documents. The searcher could use these lists to create a more restricted or expanded set of queries. The searcher could also selectively view images of documents from these lists.

Three sources of electronic documents stored within the IDSS would be available to a document searcher. First, there would be classified electronic documents that would be stored locally at the searcher's agency. These documents would be available only to that agency. Second, there would be unclassified documents stored locally at the agency. These would include documents that had been fully declassified by the agency or those that were unclassified because any remaining classified parts within the documents had been excised. These documents would be available to the local agency and to other agencies via an Internet connection. The third source of electronic documents available to a searcher at one agency would be unclassified documents stored at other agencies that had been made available via the Internet.

As with paper documents selected for review, the document searcher would inform the IDSS that a set of relevant electronic documents had been found. The IDSS would assign document numbers and associate the documents with the current case. Once the set of documents had been selected, the IDSS would enter the case into a document review queue for processing by document reviewers.

The document reviewers would continue processing a case in several ways: they would view electronic documents selected by the document searchers, they would look at paper documents that could not be scanned (when necessary), they would refer documents to other agencies for review, and they would declassify documents in whole or in part and submit these declassified documents for dissemination. Document reviewers also would respond to requests to review documents submitted by other agencies. Review can be a one- or two-step process. In the one-step process, the single reviewer has declassification authority. In the two-step process (currently used in many agencies), the initial reviewer makes recommendations to a final reviewer who has declassification authority. The IDSS would support both of these processes. When all documents for a case had been reviewed and responses to all referrals had been received, the IDSS would enter the case in the document dissemination queue.

Document dissemination staff would start the final processing step of a case by preparing redacted documents for dissemination, which would consist of completely obliterating material contained within excision boxes and removing any sticky notes that the reviewers might have attached to the document. The IDSS could turn the area within the excision boxes all black or all white and the boxes could be outlined or not. The decision on excision appearance would be agency-specific. The next step would be to reapply OCR conversion to the redacted documents. This last step would assure that no text material formerly inside excision boxes would appear in the converted text. The IDSS would do the obliteration of excision boxes and reapplication of OCR conversion automatically when a case was selected for final processing. Using the IDSS, the dissemination staff would view all pages with excision boxes before printing or storage in unclassified databases.

The steps outlined in the preceding concept of operation discussion would have been executed on the classified component of the IDSS. The steps discussed below would be performed on the unclassified component of the IDSS after the case and its declassified and/or redacted documents had been transferred to this unclassified component.

The unclassified component of the IDSS would be used to prepare a response letter to the original requester, noting as attachments the documents that

were declassified or redacted to fulfill the request. Dissemination staff could add comments to the letter as necessary and instruct the system to print the final response package, which would consist of the letter and any attached documents. Using the IDSS, the staff could also print copies of the released documents for reading rooms and send electronic copies for the unclassified databases.

Conclusions and Recommendations

There is a need for greater automation to support agencies' declassification activities. Many agencies have substantial backlogs of information requests because they have insufficient staff and automated support to respond to requests on a timely basis. IDSS implementation by agencies would provide the much-needed automated support in document searching, reviewing, redacting, and disseminating information. (Some agencies have already implemented, or are in the process of implementing, similar systems.)

We recommend that agencies give priority to automated support for their declassification activities to accomplish the Administration's objective of expediting declassification. Agencies should facilitate the future review, and general access to, their newly created documents by organizing them in electronic databases and indexing them for ready retrieval.

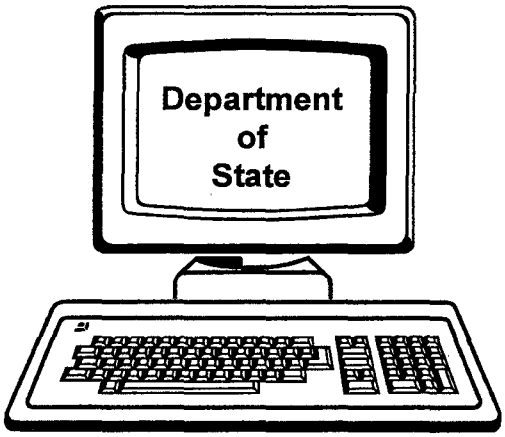
As currently planned, the Government Information Locator Service (GILS) initiative will call for agencies to provide access to catalogs of their unclassified documents. The recommendations listed below are based on the assumption that agencies will cooperate in establishing an interagency database of declassified information that will go beyond the GILS requirements by including the contents of documents:

- Agencies should agree on the contents of the interagency database, standards for interchange of information, and how the database will be developed and maintained.
- A detailed plan should be developed for implementing the interagency database.
- The database of declassified documents should be distributed among participating agencies with each agency maintaining its own portion.
- The distributed database should be interconnected through the Internet.
- There should be a prototype development of IDSS. The developer should furnish all participating agencies with the resultant custom software, to avoid duplication of effort and expense in implementation.

Howard E. Clark is a Group Leader, Glenn P. Cooley is a member of the Technical Staff, and Rex C. Klopfenstein is a Lead Engineer of The MITRE Corporation, which completed an extensive study of Executive Branch agency needs for automation support for their declassification programs in the fall of 1994.

Sources

1. *Information Security Oversight Office, 23 March 1994, 1993 Report to the President, Information Security Oversight Office, 750 17th Street NW, Suite 530, Washington, DC 20006.*
2. *H. E. Clark et al, October 1994, Interagency Declassification Support System: Estimated Costs and Implementation Considerations, MITRE Technical Report 94W101, The MITRE Corporation, 7525 Colshire Drive, McLean, VA 22102.*



FREEDOMS: DEPARTMENT OF STATE INFORMATION AUTOMATION EFFORTS

"**FREEDOMS**" is the acronym for the Department of State "**FREE**dom of Information **DO**cument **M**anagement **S**ystem" automation efforts under the direction of State's Office of Freedom of Information, Privacy, and Classification Review (FPC). This umbrella concept [see **Figure 1**] incorporates five distinct, yet integrated, systems that facilitate processing of information requests and then permits the widest possible dissemination of their outputs. **FREEDOMS** not only represents the culmination of fifteen years of incremental growth in automated information processing in the Department's Bureau of Administration, but it also points the way toward better customer service. This will be accomplished through integration of **FREEDOMS** with **"OASYS"** (the new **A**uto-Indexing/Retrieval **SYS**tem) which will combine FPC's information request processing capability with access to the Department's official foreign affairs data base of documents.

FREEDOMS is an officially mandated system designed to allow the Department of State to process and track requests for information quickly, efficiently, and with a high degree of confidence. The system works equally well for requests received under US information access laws and for special research projects undertaken by State at the direction of The Congress, the Justice Department, the Office of Management and Budget, other Executive Branch agencies, or the White House. Thus, the Department considers it a mission-critical system with many attractive attributes:

- •Maximizes limited fiscal and human resources
- •Minimizes redundancies of function within State
- •Enhances cooperation with other agencies
- •Integrates management of statutory information needs
- •Employs business process reengineering studies
- •Focuses on working smarter rather than just harder
- •Improves service to the customer
- •Supports objectives of the National Program Review
- •Conforms with the National Information Infrastructure
- •Serves as model for government-wide systems
- •Provides State-owned software for other agencies

FREEDOMS is also an integral part of FPC's short- and long-range Management Plan and will provide one of State's key links to the Information Super-Highway. In light of The MITRE Corporation feasibility study concerning the Interagency Declassification Support System, a major capability is the role **FREEDOMS** will play in the Department's declassification and release of official information into the public domain.

The initial advantage of **FREEDOMS** is to improve FPC responsiveness to customers by applying automated technology to facilitate case processing. Each of the five subsystems must interact smoothly to accomplish this.

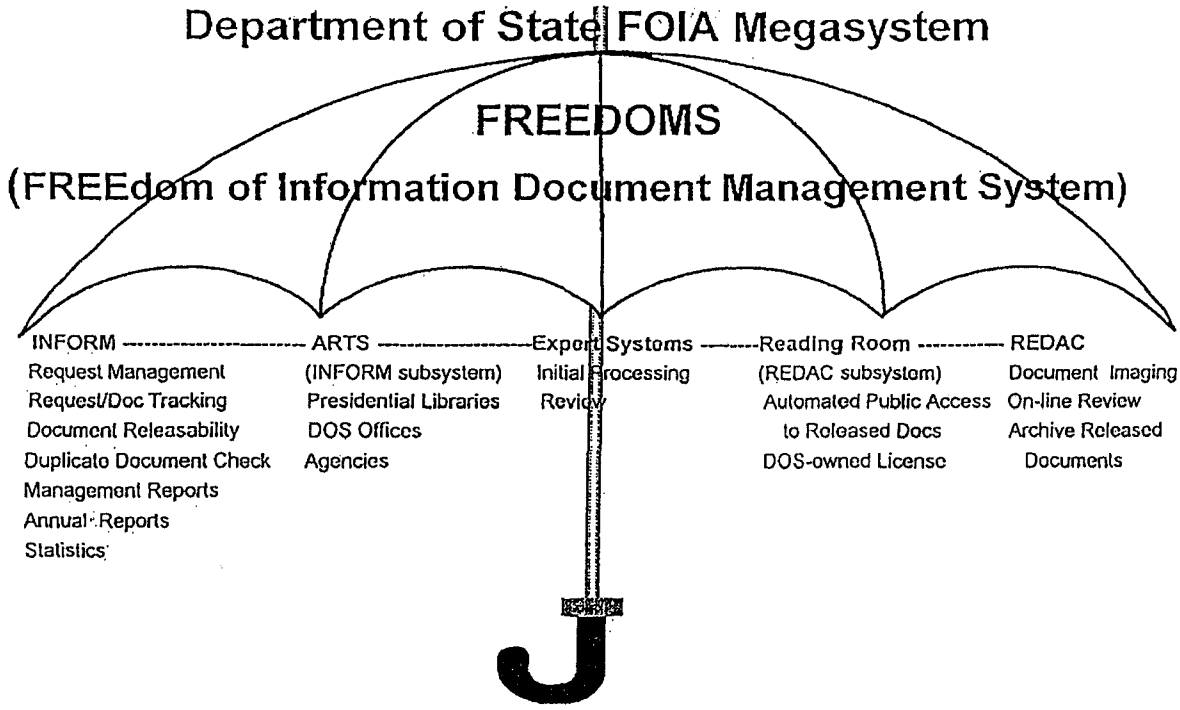
Here are the five subsystems that comprise **FREEDOMS:**

INFORM--INFOrmation **R**equest **M**anagement

The INFORM subsystem was initially developed about 1980 but still serves as the means for tracking all of the Department's cases. It contains a record of all requests for access to State information and also maintains the central index to all classification and declassification actions taken after review in response to these requests. INFORM provides statistics on workloads, backlogs, performance, review actions, and the sources and types of information requested and released; it also allows reviewers to check for documents previously reviewed to avoid unnecessary duplication of efforts.

An extensive business process reengineering study was conducted for FPC, resulting in a complete redesign of INFORM. The new subsystem will be more user-friendly, more open-system compliant, and more readily compatible within the community of Federal Government systems. When this redesign is completed, INFORM will be even more flexible in adapting a wide variety of enhancements and refinements to respond to legislative and program requirements, and will be able to produce ad hoc reports responsive to management needs. In addition, the proposed links with the corporate data base will allow State the means to ensure that the data base reflects the current classification of requested documents; the links will also facilitate transferring documents from the corporate data base into REDAC and INFORM electronically where possible.

Figure 1



ARTS--Automated **R**equest **T**racking **S**ystem

ARTS is a subsystem of INFORM that was designed to perform very simple case-tracking and document listing functions. It was initially installed in a pilot mode in several bureaus of the Department to permit internal case tracking and to create document lists which are then downloaded to diskette. These are next forwarded to FPC, along with documents that satisfy the information request, for uploading into INFORM.

An earlier version of ARTS was developed for use by the Presidential Libraries (PLIS--Presidential Library Information System) to facilitate the processing of mandatory review requests for documents from their collections. PLIS and ARTS enable the Libraries to create cases and to list the documents requested. Staff members download the information and forward the diskette along with the documents for review by the Department--or by any other agency with similar software. Obviously, using diskettes avoids time-consuming and labor-intensive rekeying. The main purpose of the ARTS and PLIS is to standardize data fields to enable electronic, inter-agency transfer of information, a basic step toward developing an inter-gency data base of declassified documents that can be easily searched by public users, possibly via the Internet.

REDAC--Freedom of Information Document Imaging System

REDAC is a commercially-produced package designed to meet the needs of Freedom of Information Act (FOIA) offices. It provides an imaging and redaction capability for scanning texts of documents into an image format which remains unchanged throughout the review process. Deletion of classified and other protected text is accomplished by creating electronic "overlays" on which reviewers indicate their deletions, reasons for deciding to excise text, and other comments pertinent to this process. Overlays and the documents are stored permanently for future reference.

A senior reviewer checks the work of reviewers and, when satisfied with the decisions, forwards results to action officers for final response to the requester. The user can print three versions of the reviewed document:

1. Original, as scanned into the image without modifications or overlays.
2. Requester, with deleted information whited- or blacked-out and FOIA exemption categories indicated.
3. Department of Justice, showing all the original text with excised areas highlighted and the FOIA exemption categories identified.

It goes without saying that the "Requester" version is unclassified and releasable to the public, while the other two must remain protected for one or more reasons (e.g., classified).

REDAC is expected to be fully integrated with INFORM and to provide linkage to the State Department central document data base. This will permit

direct downloading of designated cable texts from the central data base on to the REDAC workstations, eliminating the steps of producing paper copies and then scanning them for REDAC reviewers.

Reading Room--Stand-alone Subsystem of REDAC

The Reading Room contains copies of sanitized or declassified documents released into the public domain under the Department of State public access program. The data base can be searched by subject or by document title. Currently, public access is possible on a walk-in basis; future potential access will be via a dial-up capability using a Government or commercial-wide area network such as Internet. Department of State officials view Reading Room as the foundation for, or part of, the Interagency Declassification Support system public access data base proposed by The MITRE Corporation and mandated by Executive Order 12958 of 17 April 1995.

Expert Systems--On-line Assistance for Decision-Making

FPC has embarked on an ambitious project to develop expert systems which will aid officials processing requests for documents. These decision-support systems will ensure that processing is consistent and complete. They will also provide help and supporting documentation (e.g., procedures manuals) on-line to officials who open, process, or close cases. FPC looks to Expert Systems to reduce the burden of training new personnel by providing user-friendly support and on-line help for all aspects of case processing. Expert Systems will also empower employees by supplying them with high-level expertise on their desktops--literally at their fingertips.

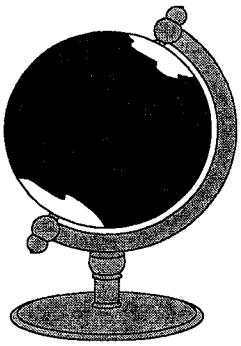
Measuring customer satisfaction is important to ensure that the Department of State has met the needs of requesters. FPC intends to address this concern in a forthright manner. In conjunction with State's ongoing efforts to ascertain the level of service provided to its customers, FPC will employ survey software to construct simple on-line questionnaires for the Reading Room to obtain feedback on user reactions to, and level of satisfaction with, the ease of use and efficiency of Reading Room operations. State may also print a similar questionnaire to send to requesters to evaluate user satisfaction with case processing efforts.

State continues to upgrade **FREEDOMS** to ensure that systems are flexible and compatible with other configurations within the Department and throughout the Federal government. Plans call for installing an optical character reader with full text indexing and retrieval capability on the front end of the imaging subsystem. This will ensure that State captures the essence of the documents and will reduce the necessity for human indexing and other process-slowing interventions. Reading Room users can then be offered the widest possible scope of text for information search, and they have an increased possibility of locating exactly the information needed.

FPC also cooperates with other agencies in working toward developing common standards for document identification and case tracking. This will facilitate electronic exchange of data and reduce, if not entirely eliminate, dependence on paper and requirements to rekey the data. Over the past several years, the Department of State has become the focal point for questions referred by the Office of Management and Budget, the National Archives, and others informed about automated information processing and imaging capability. State provides briefings and demonstrations on **FREEDOMS** to representatives from Federal agencies; foreign, state, and local governments; and other interested parties. The constant theme is system compatibility throughout the Federal Government for ease of data exchange, for rapid and accurate service to the customer, for the preservation of permanent records for archival purposes, and for dissemination of information to the widest possible audience.

With the exception of REDAC, all **FREEDOMS** subsystems are owned by the Department of State and may be made available for use free of charge to other Federal Government agencies which do not currently have automated case tracking etc systems. State is looking to update REDAC with an enhanced tool set, possibly even with a package that can be freely shared with other agencies. To date, subsystems have been provided to the National Archives, the US Navy Historical Center, and an office of the Department of Agriculture.

This description of the Department of State automated information processing capability is based upon material provided by Ms. Jacqui Lilly, Chief of the Technology Application Branch of the Department of State support staff, who concurred in the final draft of this article.



LEGACY PROJECT PRODUCES DECLASSIFICATION MODEL JUST IN TIME FOR EXECUTIVE ORDER

Ella Nargele
Ron Benjamin

In 1993 two events occurred which could have a great impact on the Naval Historical Center (NHC or Center) archives. At the time, however, there was little awareness of the congruence of the intent behind the two events.

The first of these was receipt by NHC of a grant from the Department of Defense (DoD) Legacy Resource Management Program to develop an automated declassification methodology for U.S. Navy Cold War records that could be a model for the Defense community. The Center selected its large collection of Vietnam-era records for the demonstration project.

The Legacy program was established under the DoD Appropriations Act of 1991 to identify, protect, and enhance the many irreplaceable biological, cultural, and geophysical resources found on military installations. Preservation of Cold War culture was included almost as an afterthought, but this section provided the opportunity for the Center to apply for the grant.

The second event involved inclusion of declassification language in the Clinton Administration revised draft National Security Information (NSI) Executive Order (EO). It intended to end the secrecy that has been a legacy of the Cold War, and to bring about a greater aura of openness in government. The new EO will automatically declassify most twenty-five year old records unless agencies act to retain their security protection.

Each of these efforts encountered unexpected problems and delays, but the President signed the "Classified National Security Information" EO on 17 April 1995, and the NHC declassification project completed operational testing that same week. The automated processes developed by the NHC to aid reviewers show great promise in providing for a means to implement declassification review requirements of the EO.

The NHC started its Legacy project by engaging the services of an experienced declassification consultant who researched state-of-the-art hardware and software adaptable for the creation of a declassification program and database. The system had to meet the following requirements:

- Capacity for holding large volumes of classification guidance
- Software able to perform rapid full text search of selected topics or information
- Textual input via optical scanning, floppy disk, or keyboard
- Indexing, tracking, and accounting of declassification and review activity
- Desktop-to-desktop secure inter-agency coordination of issues using compatible formats
- Flexibility and capacity to accommodate future requirements relating to the EO, Freedom of Information Act, and other public access laws or regulations.

After much coordination with DoD procurement officials, NHC selected a UNIX platform and PixTex/ Electronic Filing Software (EFS) from Excalibur Technologies Corporation. The system provides versatile document capture, flexible document storage and fast and easy document retrieval. Conceptually it works like an ordinary filing system with file cabinets, drawers and folders. Considerable effort by the contractor and NHC resulted in the development of specific procedures and local applications that could benefit other users of similar systems.

The central collection of classification guidance managed by the Navy Information Security Policy Office was crucial to creating this vital database. Approximately 640 available classification guides were easily loaded into the NHC system by disk, leaving plenty of capacity for more to be added later. A list of centrally-managed original classification authorities (OCAs) obtained from the Navy Information Security Policy Office also helped in developing points of contact for issues that the project consultant knew from experience would arise.

The team also examined their records in the NHC Vietnam-era holdings to determine their content. They surfaced numerous glossaries of terms, acronyms, and abbreviations that will help declassifiers understand information in the documents being reviewed. Interviews with Vietnam subject matter experts and informative data obtained from Presidential Libraries and the other Military Services enhanced the team's efforts to locate pertinent aids. Those efforts continued throughout the project to ensure that no terms or information with classification implications would be overlooked.

The project team established critical points-of-contact (POC) within DoD, the Services, and other

Government agencies through personal visits and/or telephone. They contacted twenty-five separate offices to explain the project and seek assistance in resolving issues and equities that fell within their area of responsibility or expertise. The team also requested any current guidance relating to the Vietnam era that could update or add to the existing Navy guidance. They agreed to coordinate issues via secure fax and voice. Once POCs understood the intent of the project, their initial fears or resistance were replaced by enthusiasm and high-level support.

By this time the project had moved beyond the conceptual stage. The project team loaded information into a database. Navy guidance was loaded by disk; glossaries of terms, acronyms, and abbreviations by optical scanning; and OCA and POC information by keyboard. They also entered other helpful data from Presidential Libraries and other Services and agencies by optical scanning and keyboard. The team surveyed NHC Vietnam records and selected documents for operational testing. Results were gratifying and immediately successful.

Once the NHC Declassification Officer was trained, the system attained operational status. To operate the system, the declassifier enters topics related to classified items and the system performs its rapid search routines. It displays possible sources of guidance which the declassifier can easily retrieve and analyze [See **Figure 1**]. The declassifier can either make a classification decision immediately or, when guidance requires, refer the issue to the cognizant OCA for resolution.

When guidance is vague or not available, especially for information classified by another agency, declassifiers can send issues to an OCA for resolution and, when appropriate, request "limited declassification review authority" for similar subject matter to be reviewed in the future. If such authority is granted in writing, the declassifier will enter the decision into the system and use it as guidance and avoid wasteful repetitive referrals to the OCA.

To refer an issue to the OCA, the declassifier displays a standardized "inquiry format screen" [see **Figure 2**] and fills in the blanks showing OCA information, the issue, the recommendation, and space for a reply. Under some circumstances, this inquiry can be sent to the responsible agency electronically. The system tracking software automatically keeps a history of work on the document and indexes it by its archive collection title; it automatically gathers data for reports such as the annual report to the Information Security Oversight Office (ISOO) showing number of cases and documents handled, pages released, and pages denied [See **Figure 3**].

The new EO mandates automatic declassification, after a five year period, of all records of permanent historical value that are over twenty-five years old. The only exceptions are those records containing information specifically exempted by the Order. Classified information approaching the twenty-five year date will also be subject to automatic declassification and consequently add to the impact of the Order. Within 180 days of the signing of the EO, agencies must notify the President of specific file series of records for which review has determined that the information in those files almost invariably falls in one or more of the handful of exemption categories. They must also send a compliance action plan to ISOO. In discussions with OCAs and other POCs, the project team has discovered that many agencies have only begun planning for these actions. This demonstration project was conducted to help agencies save time and effort by serving as a model for comparative purposes.

The EO requires several time-sensitive actions which could be accommodated by the capabilities of the NHC model:

1. Rapid Reference to Classification Guidance

Users can load this into the system in any logical manner using subject files and sub-files. They can also add modifications or clarifications to the list of exempted file series as well as inter-agency guidelines. Guidance can easily be added or changed as new information becomes available. POC and OCA lists, thesauri, codewords, terms, abbreviations, and acronyms would complement and facilitate the use of other information.

2. Secure Communications

Reviewers desiring to refer issues or equities to other organizations can easily and securely transmit them from their workstation to a distant facsimile machine or remote workstation, and receive a reply in similar fashion. This reduces the time spent using secure voice or fax-to-fax links for coordination.

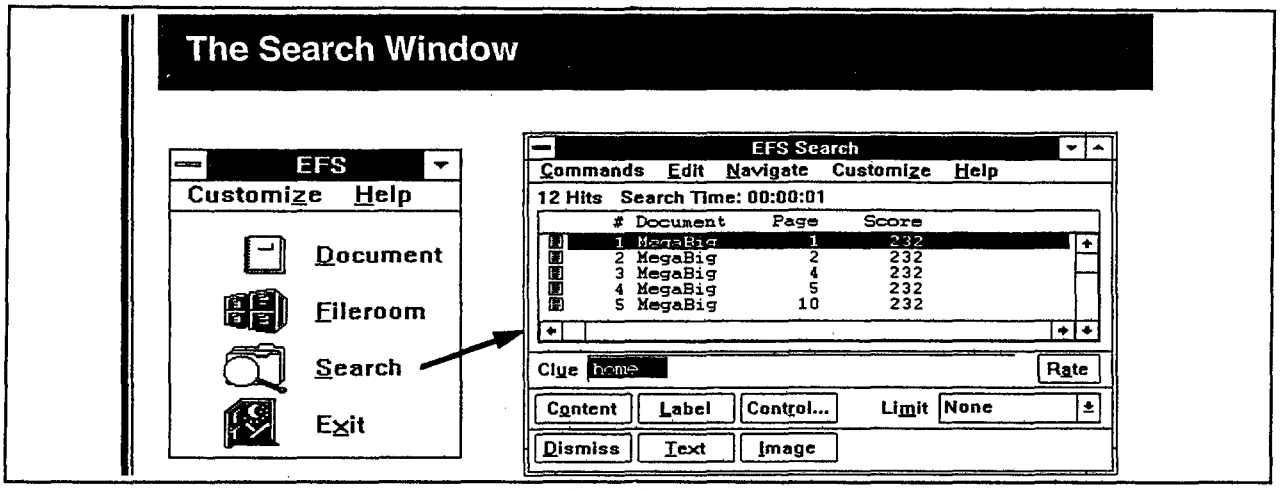
3. Redaction

Although not required for this project, redaction is essential to the declassification and review processes. Certain software can be used with the PixTex software to provide this capability on-screen during the review process leaving the original image protected while preparing the redacted copy for release. Proper redaction techniques will protect all classified or withheld information from disclosure to unauthorized persons, and allow for easy means of affixing to a document an exemption citation or rationale statement for the redacted portion.

4. Tracking System

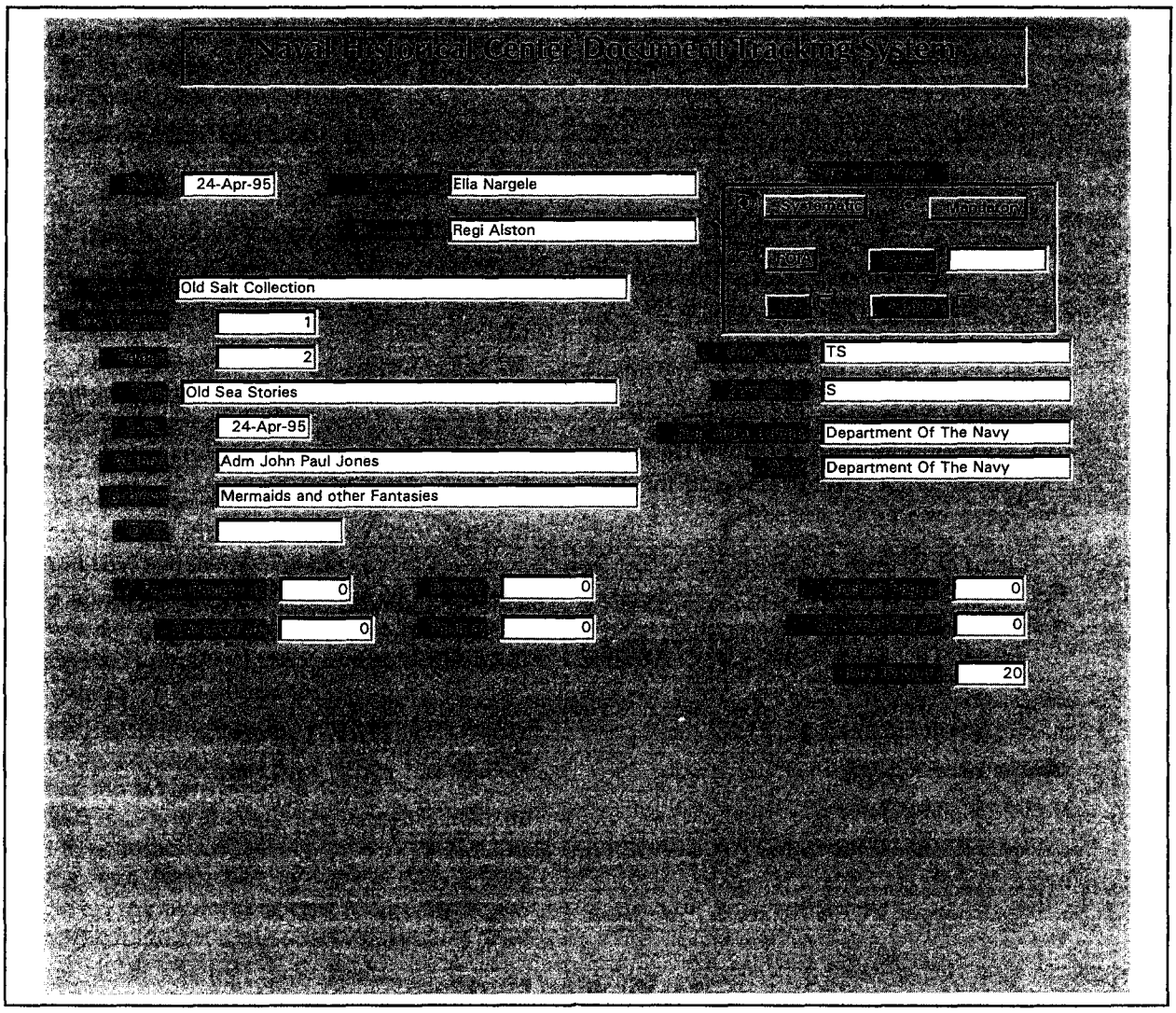
This function ties the whole process together by keeping a record of all work on a document, providing

Figure 1



Using the EFS Search Window to locate a topic within the database.

Figure 3



Document Information Form. Information is placed in this form to index the information and track the declassification process.

Figure 2

(Classification Marking)

From: Naval Historical Center
Declassification Officer
Washington Navy Yard
901 M Street SE
Washington DC 20374-5060

ISSUES/EQUITIES

POC: Department Of The Navy

Classif: S / WN / NF

IssueID: 20-1

Name: Mr. Cal B. Cavalcante

Sent: 09-May-95

Title: Chief Archivist

Operational Archives Branch

Voice: (202) 555-1000 FAX: (202) 555-1010

STU III: (202) 555-1005 SecureFAX: (202) 555-1011

Action Item:

Recomend:

Response:

The above referenced sensitive issue is contained in a Historical Naval Document. The document is being reviewed for Declassification. Please let me know if this issue can be declassified.

Return this form to me with your determination. It can be sent by secure fax to one of the numbers shown above. .

NOTE - THIS IS NOT A CLASSIFIED DOCUMENT!

Voice: (202) 433-3170 **Fax:** (202) 433-3593

Secure Voice: (202) **Secure Fax:** (202) 685-0047

NOTE - THIS IS NOT A CLASSIFIED DOCUMENT!

(Classification Marking)

Issues and Equities Screen is used to resolve issues with POC's.

indexing by collection or series, identifying and transmitting issues for resolution, entering resolved issues (with written OCA permission) for future guidance, and gathering information for data reporting requirements.

Conclusions

The project team deems the following as key lessons learned and, when combined with the above discussion, should stimulate thought for planners of declassification and review systems:

- Meeting DoD procurement policies impedes system development and adds to overall costs.
- Agencies heavily involved in classification management tend to be protective because of their belief that their own information is more sensitive than that of other agencies. This causes agencies to be cautious about cooperating with other reviewers.
- Up-to-date declassification guidelines and POC lists are absolutely essential.
- Secure electronic intra- and inter-agency communications are the key for rapid resolution of issues.
- Computer system processes must be simple and user-friendly for the declassifier. Automated processes must work for the user, not vice versa.
- Optical scanning "eats" memory; unless you need the ability to view other images, scan only those files requiring redaction.
- Input text data by disk if possible because it saves memory.
- A requirement exists for more functional redaction software that is versatile enough for use with any software. At the present time no standard exists because of the limited demand for redaction software.
- OCAs can use the system in training their personnel to declassify documents.
- Automation is essential for future declassification activities because its greater efficiency can result in decreased time and money spent.
- Creation of a database of declassified and unclassified documents for the use of researchers requires the development of an archival arrangement of the records prior to creation of the database.

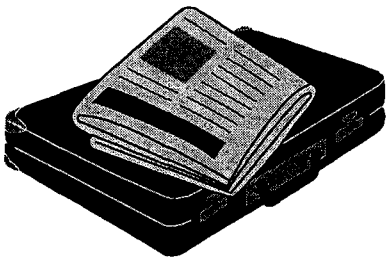
The Navy system was designed for a small operation but can be expanded as necessary. In its present configuration the system provides for up to 64 concurrent workstations and the storage capacity can be expanded to accomodate the entire NHC holdings of 65,000 cubic feet. Redaction software is easy to add. Workstation to remote workstations, secure communications and coordination is our near term primary goal.

This methodology will enable the NHC to release declassified information in a more timely manner and is a candidate to serve as a model for other DoD and Federal Government agencies. It conforms to the MITRE recommendations for automated declassification systems* and the sharing of information among agencies once it is declassified and released to the public. Further, this database marks the beginning of a Navy directory of declassification actions. Enhancements currently underway include computer-to-secure fax and computer-to-computer capability in cooperation with the Air Force, which is developing a similar system. This should help enhance the credibility of the Government because the system serves researchers, historians, and the general public by enabling declassifiers in one agency to release groups of records in their entirety. It will also help agencies protect their classified information from premature release.

Ella Nargele conducts systematic and mandatory declassification reviews of Navy historical records and in response to FOIA requests at the Naval Historical Center. She is the program manager of the declassification model project.

Ron Benjamin is a management consultant with Security Classification & Review, Inc. and a member of the project team. He is a retired Air Force Reserve Colonel who previously served as a Senior Advisor to the Secretary of the Air Force's Declassification and Review Team.

**MITRE conducted research into the feasibility of a compatible Inter-agency Declassification Support System (IDSS)*



VIRTUAL INTERVIEW WITH THE DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE

Q: *Congratulations upon completing a lengthy and difficult process to issue a new executive order governing classified information! How has this process differed from your experience leading up to issuance of Executive Order (EO) 12356, the current policy document, in April 1982?*

Answer: To answer this question, I must admit that I'm saving the really good stuff for my book, Confessions of a Federal Bureaucrat: Security Official and Lawyer, which I'll write in retirement. The empathy and excitement inherent in the title assure a best seller.

In working on this Order and its predecessors, I note one clear similarity: the belief going in by persons new to this subject area that the process will be much easier and quicker than it turns out to be. Although relatively few Americans take much interest in the subject of national security secrecy, those who do are most passionate in their views. These passions, and the importance of the subject matter, make it very difficult to resolve disputes quickly or to arrive at reasonable compromises.

Perhaps the most significant difference from the process that resulted in EO 12356 was the continuing interest and involvement of top White House officials, including persons outside the National Security Council staff. Obviously, interest at such a level tends to delay the resolution of disputes, because other matters of national security concern often involve crisis management situations and understandably take priority.

Q: *What were some of the problems EO 12356 created for Federal agencies, classifiers, declassifiers, the National Archives, private citizens, special interest groups, and others that gave rise to the issuance of EO 12958?*

Answer: In my view, the major failing of all our security classification systems up to now has been the absence of a viable declassification program that could adequately address the huge build-up of older, permanently valuable classified records. The overuse of the "OADR" instruction has exacerbated this problem under EO 12356. However, the major reason for the huge build-up in recent years is the universality of technology that allows for the almost effortless reproduction and transmission of information, including classified information, when people fail to exercise restraint.

Q: *In view of these problems, what do you consider to be the strengths of EO 12958?*

Answer: The major reform of EO 12958 is the introduction of an automatic declassification provision that clearly shifts the resource burden in favor of declassification. Under EO 12356 and its predecessors, in order to declassify any information, including older information, an agency was obligated to devote money and human resources to the laborious process of page by page review. Otherwise, the information remained classified. Under EO 12958, the resource burden has shifted 180°. If an agency wants to keep older information classified, it must devote resources to the process to demonstrate how the information falls within an exemption to automatic declassification. Otherwise, permanently valuable classified information is automatically declassified when it becomes 25 years old.

Over the past several years, we have been talking a great deal about risk management. The declassification program under EO 12958 will truly constitute an example of risk management in practice, not just words.

Q: *One of the consequences of the Presidential Review Directive 29 Task Force was broader communications among security specialists in some two dozen Federal agencies. Is it fair to ask whether EO 12958 has an objective of achieving greater uniformity in classification, safeguarding, and declassification policy among these agencies; that is, will we be working toward a truly "national" National Security Information program?*

Answer:

Yes, it is fair to ask that question. Answering it is more difficult.

Greater uniformity is an important objective of EO 12958. To achieve this objective, I believe that the implementing directives must strive for as much standardization as is feasible, cost effective and efficient. However, because the implementing directives establish standards that the agencies must achieve at a minimum, we cannot be totally inflexible. For example, agencies should have reasonable alternatives for the storage of "Confidential" information, consistent with existing inventories, costs, and the degree of protection provided by various security containers. We should not forbid the use of class 5 or class 6 containers to store "Confidential" information. But if we require the use of class 5 or class 6 containers to store all "Confidential" information, the overall costs of storage will skyrocket. On the other hand, it is absurd to permit differences that exist merely for the sake of being different. For example, why should an agency dictate what specific

color an overall classification marking should be on its classified documents?

Q: *From the standpoint of the security specialist, what are the major security policy differences introduced by EO 12958?*

Answer:

There are over 70 substantive differences between EO 12958 and EO 12356. A good security specialist or classification manager won't need to be able to list them. However, he or she must become familiar enough with EO 12958 to be fully comfortable in briefing others about it; and to know when he or she really doesn't know the answer to a question, but knows how to find that answer.

Without trying to be exhaustive, I consider the following new or revised areas as critical to the knowledge and skills of an effective security classification specialist under EO 12958: (a) understanding and explaining to others the differences between the 10-year rule for duration of classification and the 25-year rule for declassification; (b) being familiar with the agency's system for challenging the classification of information; (c) being able to train or brief an original classification authority on the essential elements of original classification; (d) understanding the purpose and application of the "classified why" line; (e) being able to assess and critique a classification guide or declassification guide; (f) conducting an effective review of an organization's classified product; (g) estimating reasonably the costs of the security classification system within the individual's organization; and (h) establishing oneself as a critical and reliable resource to top management.

Q: *What changes do you foresee in the way original classification authorities go about the task of making decisions under the new Order?*

Answer:

In a number of its provisions, including performance evaluations, EO 12958 clearly emphasizes individual accountability for original classification decisions. The original classification authority, whether acting directly or through an aide, must recognize the responsibilities and consequences associated with the act of original classification. We must insist on original classification by reasoned thought, not by rote, or fear, or embarrassment.

All too often in the past and present, agency officials have "excused" original classifiers from receiving training on their responsibilities because they were too high up in the chain of command to be bothered. That is why this is the first Executive Order that specifically mandates the training of original classifiers. The necessary training need not be burdensome nor lengthy, and can, with all the technologies available to us, be designed to fit the needs and schedule of the busy executive.

Q: *How will derivative classifiers throughout the Federal Government and industry change the way they determine the classification levels of information or mark documents under EO 12958?*

Answer:

As is currently the case, derivative classifiers will be bound to honor and carry forward the instructions of the original classifier. They will, however, be encouraged and expected to challenge what they believe to be improper classification through established procedures that mandate non-retribution. Moreover, by requiring the issuance of a directive on classification guides and mandating the creation of classification guides for all ongoing classified programs, we hope that the overall quality of classification guides will improve significantly. We should not tolerate or approve guides that have the effect of shifting the decision-making responsibility from the original classifier to the guide's user.

Q: *Does this new Order place information at risk by automatically declassifying it within 25 years after it was first classified, specifically that in the National Archives?*

Answer:

As I noted in an answer to a previous question, the automatic declassification provision is, in my view, a reasonable exercise of risk management principles. We know from many years of experience that well over 90% of 30-year old classified information is declassified upon review. I believe agencies will need to distinguish and review quite differently three distinct groups of records: (1) those that are replete with information that may be exempted from declassification after 25 years; (2) those that are unlikely to contain exempt information; and (3) those that are likely to contain some exempt information within largely non-exempt material. The correct allocation of resources among these three basic groups of records will be critical. The third group will require the greatest allocation of resources.

I don't believe that the level of risk increases based on the location of the information within the National Archives. As a matter of fact, one of the first things agencies need to get a handle on is what records are affected by the automatic declassification provision. Perhaps the most easily identified are those already in the National Archives.

Q: *Will the new EO change the way we handle or mark foreign government information, or the way they deal with ours?*

Answer:

There are three important changes in EO 12958 with respect to foreign government information (FGI). First, both EO 12356 and EO 12958 define FGI as information provided by a foreign government or organization of governments with the expectation of confidentiality. In EO 12958, however, the modifying words, "expressed or

implied," which appear in EO 12356 after the word "expectation," do not appear.

Second, the new Executive Order does not "presume" that any category of information is classified. To be classified, the information must meet all the standards for original classification set forth in Section 1.2 of the Order. In EO 12356, however, FGI presumptively met the standards for classification simply because it was FGI. This presumption of classification in EO 12356 also applied to intelligence sources and methods.

Third, and probably most important in terms of its prospective impact, EO 12958 authorizes the safeguarding of all FGI in a manner equivalent to that required by the foreign government. Until now, we have been required to safeguard FGI that the foreign government classified at levels below U.S. "Confidential" under standards that applied, at a minimum, to U.S. "Confidential". When the new Order becomes effective, we will be able to protect low-level FGI, when equivalent to the foreign government's standards, in a manner that doesn't necessarily meet the standards for U.S. "Confidential". For example, we may be able to store this information in a locked desk rather than in a security container. Perhaps most significant, we may be able to grant access to certain low-level FGI to a person who does not otherwise have a security clearance.

Q: *If you could have made one uncontested change in how the U.S. has conducted its information security programs over the past 50 years, what would you have had us do differently?*

Answer:

On the whole, I think we can be most proud of our information security practices and programs over the past 50 years. I know from my conversations with representatives of foreign governments and foreign journalists that our commitment to open government and public access to information is unparalleled and unprecedented. At the same time, the systems and programs have worked to protect our national security interests. Where they have failed is when individuals, most of them appropriately recognized as criminals, have taken it upon themselves to violate these systems and programs.

There remain several areas that seem permanently outside the reach of the most well-intentioned draftsman. One of them is coming up with a fully plausible system that routinely and correctly answers the question, "How long must information remain classified in order to protect our national security interests not a moment too short and not a moment too long?" While that may seem like a preposterous question, that is essentially what our security classification system calls for us to answer.

There is one boring piece of practical advice that now seems so obvious, but which we have clearly ignored over the years. We must integrate classification management more closely with information and records management. If we have been following that advice from the beginning, the tasks ahead of us would be far, far simpler to accomplish.

Q: *Are there other matters you wish to address so NCMS members, and other security professionals, can understand their roles in Government and industry and perhaps improve program performance?*

Answer:

EO 12958 emphasizes the importance of good classification management. I know that is recent years it has become fashionable within some quarters of NCMS to downplay its roots in classification management. To me at least, these roots, and the people associated with them, are what distinguish the Society from other organizations of security professionals, and are the reason that over the years I have turned first to NCMS for its input.

THE WHITE HOUSE
Office of the Press Secretary
For Immediate Release April 17, 1995

STATEMENT BY THE PRESIDENT

Today I have signed an Executive order reforming the Government's system of secrecy. The order will lift the veil on millions of existing documents, keep a great many future documents from ever being classified, and still maintain necessary controls over information that legitimately needs to be guarded in the interests of national security.

In issuing this order, I am seeking to bring the system for classifying, safeguarding, and declassifying national security information into line with our vision of American democracy in the post-Cold War world.

This order strikes an appropriate balance. On the one hand, it will sharply reduce the permitted level of secrecy within our Government, making available to the American people and posterity most documents of permanent historical value that were maintained in secrecy until now.

On the other, the order enables us to safeguard the information that we must hold in confidence to protect our Nation and our citizens. We must continue to protect information that is critical to the pursuit of our national security interests. There are some categories of information--for example, the war plans we may employ or the identities of clandestine human assets--that must remain protected.

This order also will reduce the sizable costs of secrecy--the tangible costs of needlessly guarding documents and the intangible costs of depriving ourselves of the fullest possible flow of information.

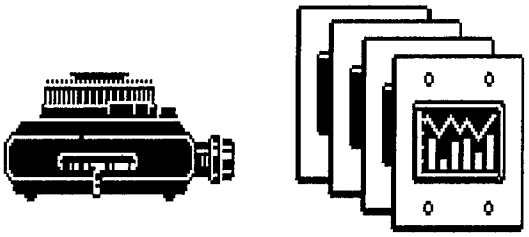
This order establishes many firsts: Classifiers will have to justify what they classify; employees will be encouraged and expected to challenge improper classification and protected from retribution for doing so; and large-scale declassification won't be dependent on the availability of individuals to conduct a line-by-line review. Rather, we will automatically declassify hundreds of millions of pages of information that were classified in the past 50 years.

Similarly, we will no longer tolerate the excesses of the current system. For example, we will resolve doubtful calls about classification in favor of keeping the information unclassified. We will not permit the reclassification of information after it has been declassified and disclosed under proper authority. We will authorize agency heads to balance the public interest in disclosure against the national security interest in making declassification decisions. And, we will no longer presumptively classify certain categories of information, whether or not the specific information otherwise meets the strict standards for classification. At the same time, however, we will maintain every necessary safeguard and procedure to assure that appropriately classified information is fully protected.

Taken together, these reforms will greatly reduce the amount of information that we classify in the first place and the amount that remains classified. Perhaps most important, the reforms will create a classification system that Americans can trust to protect our national security in a reasonable, limited, and cost-effective manner.

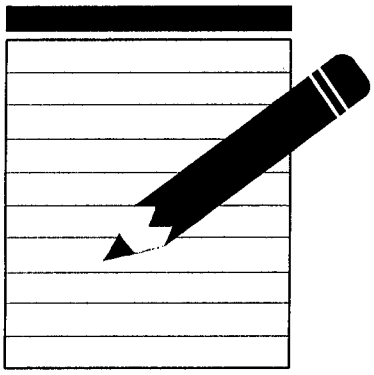
In keeping with my goals and commitments, this order was drafted in an unprecedented environment of openness. We held open hearings and benefitted from the recommendations of interested Committees of Congress and nongovernmental organizations, groups, businesses, and individuals. The order I have signed today is stronger because of the advice we received from so many sources. I thank all those who have helped to establish this new system as a model for protecting our national security within the framework of a Government of, by, and for the people.

WILLIAM J. CLINTON
THE WHITE HOUSE
April 17, 1995



HIGHLIGHTS OF THE NEW EXECUTIVE ORDER ON CLASSIFIED NATIONAL SECURITY INFORMATION

- Discourages unnecessary classification by instructing classifiers to keep information unclassified when in doubt; also directs classifiers to choose the lower level of classification when in doubt about which level is appropriate. [Sec. 1.2(b); Sec. 1.3(c)]
- Limits the duration of classification of most newly classified information to 10 years, subject to limited exceptions. [Sec. 1.6]
- Mandates automatic declassification of information that is 25 years old, unless it falls within one of the narrow exemption categories, such as revealing the identity of a human source. [Sec. 3.4]
- Establishes an Interagency Security Classification Appeals Panel to hear appeals of agency decisions on mandatory declassification review requests or challenges to classification; and to review an agency head's determination to exempt 25-year old information from automatic declassification. [Sec. 5.4]
- Authorizes agency officials to determine whether the public interest in disclosure outweighs the national security interest in maintaining classification when deciding whether to declassify information that otherwise continues to meet the standards for classification. [Sec. 3.2(b)]
- Implements a number of management improvements to better safeguard classified information and reduce the overall costs of protecting such information. [Throughout the Order]
- Stresses a general commitment to openness as a part of the classification management process. [Preamble and throughout the Order]
- Requires classifiers to identify why information is classified. [Sec. 1.7(a)]
- Eliminates presumption that any category of information is automatically classified.
- Specifies sanctions for overclassification. [Sec. 5.7]
- Requires the establishment of a Government-wide declassification database. [Sec. 3.8]
- Establishes an Information Security Policy Advisory Council of non-Government experts to recommend subject areas for systematic declassification review and to advise on classification system policies. [Sec. 5.5]
- Limits the establishment and requires annual revalidation of special access programs and increases both internal and external oversight of these programs. [Sec. 4.4]
- Requires accounting and reporting of costs associated with security classification programs. [Sec. 5.6(c)]
- Mandates training and accountability of original classification authorities. [Sec. 1.4(d); 5.6(c)]
- Calls for challenges of improper classification decisions and establishes processing procedures that ensure non-retribution. [Sec. 1.9]
- Requires personal commitment of agency heads and senior management to the effective implementation of the system. [Sec. 5.6(a)]



FACT SHEET: The new Executive Order on Classified National Security Information

Standards: Improve the Quality of Classification

The new Order:

- provides more definitions of "key" terms and places these definitions at the beginning of each major part.
- groups under one section the standards for original classification.
- requires classifiers to provide a reason for classification.
- discourages unnecessary classification by instructing classifiers to keep information unclassified when in doubt.
- retains the three levels of classification: *Top Secret*, for information the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security that the classifier is able to identify or describe; *Secret*, for serious damage; and *Confidential*, for damage.
- retains stringent limits on delegations of original classification.
- requires training of original classifiers.
- lists seven categories of information that may be classified:
  - a.) military plans, weapons systems, or operations;
  - b.) foreign government information;
  - c.) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
  - d.) foreign relations or foreign activities of the United States, including confidential sources;
  - e.) scientific, technological, or economic matters relating to the national security;
  - f.) United States Government programs for safeguarding nuclear materials or facilities; or
  - g.) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national-security.
- limits the duration of classification of most information to 10 years.
- includes the following exemptions to the 10 year rule for duration of classification:
  1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;
  2) reveal information that would assist in the development or use of weapons of mass destruction;
  3) reveal information that would impair the development or use of technology within a United States weapon system;
  4) reveal United States military plans, or national security emergency preparedness plans;
  5) reveal foreign government information;
  6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be on going for a period greater than that provided in paragraph (b) above;
  7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or
  8) violate a statute, treaty, or international agreement.
- mandates portion marking to indicate what portions are classified.
- specifies the use of a classified addendum when classified information is only a small portion of an otherwise unclassified document.
- requires agencies with original classification authority to produce classification guides for use in classifying derivatively.

Promotes Openness--Emphasizes Declassification

The new Order:

- authorizes a public interest balancing test in declassification determinations.
- calls for the automatic declassification, within five years from the issuance of the Order, of all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value.
- allows agency heads to exempt from the 25-year automatic declassification rule specific information, the release of which should be expected to:

1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of the source would clearly and demonstrably damage the national security interests of the United States;
2) reveal information that would assist in the development or use of weapons of mass destruction;
3) reveal information that would impair United States cryptologic systems or activities;
4) reveal information that would impair the application of state of the art technology within a United States weapon system;
5) reveal actual United States military war plans that remain in effect;
6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;
8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or
9) violate a statute, treaty, or international agreement.

- requires external review and approval of actions by an agency head to exempt information from 25 year automatic declassification.
- calls for the establishment of a Government-wide declassification database, and instructs the Archivist to explore other uses of technology to speed the declassification process.

Safeguarding Classified Information

The new Order:

- makes clear that the originating agency is responsible for maintaining control over classified information it generates.
- calls for the establishment of procedures to protect classified information processed on automated information systems.
- requires the annual update of distribution lists of classified information, thus curtailing the unnecessary dissemination of classified information.

Program Oversight

The new Order:

- provides that the Director of the Office of Management and Budget will issue implementing directives.
- assigns the implementation and monitorship functions to OMB's Information Security Oversight Office.
- establishes an Interagency Security Classification Appeals Panel to hear appeals of final agency decisions of mandatory declassification review requests and challenges to classification.
- establishes an Information Security Policy Advisory Council to provide ongoing expert advice on the program from non-government individuals.

Costs

The new Order requires agencies to account for the costs associated with the classification, safeguarding and declassification of information.*

*Published reports have estimated the cost of protecting national security information within government (estimated program cost of $2.3 billion) and industry (estimated program cost of $13.8 billion) at a total combined amount in excess of $16 billion per year. These estimates are based on figures contained in Office of Management and Budget's report *Cost Estimates for Classification Related Activities: FY 1994* (March 31, 1994), and *The National Industrial Security Program: A Report to the President by the Secretary of Defense* (November 1990), respectively.

EXECUTIVE ORDER 12958

CLASSIFIED NATIONAL SECURITY INFORMATION

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1 ORIGINAL CLASSIFICATION

Section 1.1. Definitions

For purposes of this order:

a.) "National security" means the national defense or foreign relations of the United States.

b.) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control""means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

c.) "Classified national security information" (hereafter classified information") means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

d.) "Foreign Government Information" means:

1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

e.) "Classification" means the act or process by which information is determined to be classified information.

f.) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

g.) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

h.) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

i.) "Agency" means any "Executive agency", as defined in 5 U.S.C. 105, and any other entity within the executive branch that comes into the possession of classified information.

j.) "Senior agency official" means the official designated by the agency head under section 5.6(c) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

k.) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

l.) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Section. 1.2. Classification Standards

a.) Information may be originally classified under the terms of this order only if all of the following conditions are met:

1) an original classification authority is classifying the information;

2) the information is owned by, produced by or for, or is under the control of the United States Government;

3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and

4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to national security and the original classification authority is able to identify or describe the damage.

b.) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

1) amplify or modify the substantive criteria or procedures for classification; or create any substantive or procedural rights subject to judicial review.

c.) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Section 1.3. Classification Levels

a.) Information may be classified at one of the following three levels:

1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

b.) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

c.) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Section 1.4. Classification Authority

a.) The authority to classify information originally may be exercised only by:

1) the President;

2) agency heads and officials designated by the President in the Federal Register; or

3) United States Government officials delegated this authority pursuant to paragraph (c), below.

b.) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

c.) Delegation of original classification authority.

1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

2) "Top Secret" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

3) "Secret" or "Confidential" original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated "Top Secret" original classification authority by the agency head.

4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

d.) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

e.) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Section 1.5. Classification Categories

Information may not be considered for classification unless it concerns:

a.) military plans, weapons systems, or operations;

b.) foreign government information;

c.) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
d.) foreign relations or foreign activities of the United States, including confidential sources;
e.) scientific, technological, or economic matters relating to the national security;
f.) United States Government programs for safeguarding nuclear materials or facilities; or
g.) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Section 1.6. Duration of Classification

a.) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b) below.
b.) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.
c.) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.
d.) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:
1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;
2) reveal information that would assist in the development or use of weapons of mass destruction;
3) reveal information that would impair the development or use of technology within a United States weapons system;
4) reveal United States military plans, or national security emergency preparedness plans;
5) reveal foreign government information;
6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;
7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or
8) violate a statute, treaty, or international agreement.
e.) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Section 1.7. Identification and Markings

a.) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in anappropriate manner:
1) one of the three classification levels defined insection 1.3 of this order;
2) the identity, by name or personal identifier and position, of the original classification authority;
3) the agency and office of origin, if not otherwise evident;
4) declassification instructions, which shall indicate one of the following:
A.) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or
B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or
C.) the exemption category from declassification, as prescribed in section 1.6(d); and
5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.
b.) Specified information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.
c.) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

d.) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

e.) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

f.) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

g.) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Section 1.8. Classification Prohibitions and Limitations

a.) In no case shall information be classified in order to:
1) conceal violations of law, inefficiency, or administrative error;
2) prevent embarrassment to a person, organization, or agency;
3) restrain competition; or
4) prevent or delay the release of information that does not require protection in the interest of national security.

b.) Basic scientific research information not clearly related to the national security may not be classified.

c.) Information may not be reclassified after it has been declassified and released to the public under proper authority.

d.) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code. Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:
1) meets the standards for classification under this order; and
2) is not otherwise revealed in the individual items of information.
As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Section 1.9. Classification Challenges

a.) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) below.

b.) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:
1) individuals are not subject to retribution for bringing such actions;
2) an opportunity is provided for review by an impartial official or panel; and
3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

PART TWO DERIVATIVE CLASSIFICATION

Section 2.1. Definitions

For purposes of this order:

a.) "Derivative classification" means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

b.) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

c.) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and estab-

lishes the level and duration of classification for each such element.

d.) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

e.) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

Section 2.2. Use of Derivative Classification

a.) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

b.) Persons who apply derivative classification markings shall:
1) observe and respect original classification decisions; and
2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:
A.) the date or event for declassification that corresponds to the longest period of classification among the sources; and
B.) a listing of these sources on or attached to the official file or record copy.

Section 2.3. Classification Guides

a.) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

b.) Each guide shall be approved personally and in writing by an official who:
1) has program or supervisory responsibility over the information or is the senior agency official; and
2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

c.) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.

PART THREE DECLASSIFICATION AND DOWNGRADING

Section 3.1. Definitions

For purposes of this order:

a.) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

b.) "Automatic declassification" means the declassification of information based solely upon:
1) the occurrence of a specific date or event as determined by the original classification authority; or
2) the expiration of a maximum time frame for duration of classification established under this order.

c.) "Declassification authority" means:
1) the official who authorized the original classification, if that official is still serving in the same position;
2) the originator's current successor in function;
3) a supervisory official of either; or
4) officials delegated declassification authority in writing by the agency head or the senior agency official.

d.) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

e.) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

f.) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

h.) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Section 3.2. Authority for Declassification

a.) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

b.) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs

the damage to national security that might reasonably be expected from disclosure. This provision does not:

1) amplify or modify the substantive criteria or procedures for classification; or

2) create any substantive or procedural rights subject to judicial review.

c.) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

d.) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Section 3.3. Transferred Information

a.) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

b.) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

c.) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

d.) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

e.) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

Section 3.4. Automatic Declassification

a.) Subject to paragraph (b), below, within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

b.) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

2) reveal information that would assist in the development or use of weapons of mass destruction;

3) reveal information that would impair U.S. cryptologic systems or activities;

4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

5) reveal actual U.S. military war plans that remain in effect;

6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;

8) reveal information that would seriously and

demonstrably impair current national security emergency preparedness plans; or

9) violate a statute, treaty, or international agreement.

c.) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

1) a description of the file series;

2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

d.) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

1) a description of the information;

2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

e.) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

f.) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

g.) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

Section 3.5. Systematic Declassification Review

a.) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order. Agencies shall prioritize the systematic review of records based upon:

1) recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or

2) the degree of researcher interest and the likelihood of declassification upon review.

b.) The Archivist shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives as of the effective date of this order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These

records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

c.) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Section 3.6. Mandatory Declassification Review

a.) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:
1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;
2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and
3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

b.) Information originated by:
1) the incumbent President;
2) the incumbent President's White House Staff;
3) committees, commissions, or boards appointed by the incumbent President; or
4) other entities within the Executive Office of the President that solely advise and assist the incumbent President are exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

c.) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

d.) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

e.) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

Section 3.7. Processing Requests and Reviews

In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

a.) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

b.) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Section 3.8. Declassification Database.

a.) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Government-wide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

b.) Agency heads shall fully cooperate with the Archivist in these efforts.

c.) Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

PART FOUR SAFEGUARDING

Section 4.1. Definitions

For purposes of this order:

a.) "Safeguarding" means measures and controls that are prescribed to protect classified information.

b.) "Access" means the ability or opportunity to gain knowledge of classified information.

c.) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

d.) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

e.) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

f.) "Network" means a system of two or more computers that can exchange data or information.

g.) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

h.) "Specific access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Section 4.2. General Restrictions on Access

a.) A person may have access to classified information provided that:
1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
2) the person has signed an approved nondisclosure agreement; and
3) the person has a need to know the information.

b.) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

c.) Classified information may not be removed from official premises without proper authorization.

d.) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

e.) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:
1) prevent access by unauthorized persons; and
2) ensure the integrity of the information.

f.) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

g.) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

h.) Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

Section 4.3. Distribution Controls

a.) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need to know the information.

b.) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Section 4.4. Special Access Programs

a.) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

1) the vulnerability of, or threat to, specific information is exceptional; and

2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or

3) the program is required by statute.

b.) Requirements and Limitations

1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

3) Special access programs shall be subject to the oversight program established under section 5.6(c) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

c.) Within 180 days after the effective date of this order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this order. Each existing special access program that an agency head or principal deputy validates shall be treated as if it were established on the effective date of this order.

d.) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Section 4.5. Access by Historical Researchers and Former Presidential Appointees

a.) The requirement in section 4.2(a)(3) of this order that access to classified information may be granted only to individuals who have a need to know the information may be waived for persons who:

1) are engaged in historical research projects; or

2) previously have occupied policy-making positions to which they were appointed by the President.

b.) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

1) determines in writing that access is consistent with the interest of national security;

2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and;

3) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

PART FIVE IMPLEMENTATION AND REVIEW

Section 5.1. Definitions

For purposes of this order:

a.) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

b.) "Violation" means:
1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;
2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or
3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

c.) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a "violation", as defined above.

Section 5.2. Program Direction

a.) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:
1) classification and marking principles;
2) agency security education and training programs;
3) agency self-inspection programs; and
4) classification and declassification guides.

b.) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

c.) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information.

Section 5.3. Information Security Oversight Office

a.) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

b.) Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs the Director of the Information Security Oversight Office shall:
1) develop directives for the implementation of this order;
2) oversee agency actions to ensure compliance with this order and its implementing directives;
3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;
4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;
5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Director of the Office of Management and Budget;
6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;
7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;
8) report at least annually to the President on the implementation of this order; and
9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Section 5.4. Interagency Security Classification Appeals Panel

a.) Establishment and Administration.
1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members.

2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.
3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.
4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.
5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.
6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

b.) Functions The panel shall:
1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order;
2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.4 of this order; and
3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order.

c.) Rules and Procedures The panel shall issue bylaws, which shall be published in the Federal Register no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:
1) the appellant has exhausted his or her administrative remedies within the responsible agency;
2) there is no current action pending on the issue within the federal courts; and
3) the information has not been the subject of review by the federal courts or the Panel within the past 2 years.

d.) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

e.) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

Section 5.5 Information Security Policy Advisory Council

a.) Establishment There is established an Information Security Policy Advisory Council ("Council"). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from among persons who have demonstrated interest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council Chair among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. 2.

b.) Functions The Council shall:
1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under this order or its implementing directives, including recommended changes to those policies;
2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and
3) serve as a forum to discuss policy issues in dispute.

c.) Meetings The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

d.) Administration
1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.
2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).
3) To the extent permitted by law and subject to the availability of funds, the Information Security Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.
4) Notwithstanding any other Executive order, the

functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the Congress, shall be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

Section 5.6. General Responsibilities

Heads of agencies that originate or handle classified information shall:

a.) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

b.) commit necessary resources to the effective implementation of the program established under this order; and

c.) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

3) establishing and maintaining security education and training programs;

4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information;

8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication; and

9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Section 5.7. Sanctions

a.) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

b.) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

2) classify or continue the classification of information in violation of this order or any implementing directive;

3) create or continue a special access program contrary to the requirements of this order; or

4) contravene any other provision of this order or its implementing directives.

c.) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

d.) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

e.) The agency head or senior agency official shall:

1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3), above, occurs.

PART SIX GENERAL PROVISIONS.

Section 6.1. General Provisions

a.) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of

1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

b.) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

c.) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b), and 5.4(e) of this order.

d.) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

Section 6.2. Effective Date

This order shall become effective 180 days from the date of this order.

THE WHITE HOUSE
April 17, 1995