Information Security Oversight Office

1994 REPORT TO THE PRESIDENT

Authority

Executive Order 12356, "National Security Information," and Executive Order 12829, "National Industrial Security Program." For FY 1995, ISOO is a component of the Office of Management and Budget/Office of Information and Regulatory Affairs. During FY 1994, ISOO was an administrative component of the United States General Services Administration, while receiving its policy and program direction from the President through the National Security Council.

Mission

ISOO oversees the security classification programs in both Government and industry and reports to the President annually on their status.

Functions

- Develops implementing directives and instructions.
- Maintains liaison with agency counterparts and conducts on-site inspections and special document reviews to monitor agency compliance.
- Develops and disseminates security education materials for Government and industry; monitors security education and training programs.
- Receives and takes action on complaints, appeals and suggestions.
- Collects and analyzes relevant statistical data, and reports them annually, along with other information, to the President.
- Serves as spokesperson to Congress, the media, special interest groups, professional organizations and the public.
- Conducts special studies on identified or potential problem areas, and develops remedial approaches for program improvement.

Goals

- To hold classification activity to the minimum necessary to protect the national security.
- To ensure the safeguarding of classified national security information in both Government and industry in a cost effective and efficient manner.
- To promote declassification and public access to information as soon as national security considerations permit.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C.

May 31, 1995

The President
The White House
Washington, DC 20500

Dear Mr. President:

We are pleased to submit the Information Security Oversight Office's 1994 Report to the President.

The past year has likely been the most important ever in matters concerning the Government-wide security classification system and program. We are delighted to report tremendous progress on several fronts. Among them:

- As noted in the data we report to you today, FY 1994 witnessed tremendous decreases in classification and significant increases in declassification. These data suggest quite dramatically that the agencies are moving beyond the Cold War in their classification practices.

  You issued Executive Order 12937 on November 10, 1994, which declassified almost 50 million pages of historical records in the National Archives.

  You issued Executive Order 12951 on February 22, 1995, which will result in the declassification and public availability of intelligence imagery.

  Most significantly, you issued Executive Order 12958, "Classified National Security Information," on April 17, 1995. This Order, which establishes the first post-Cold War security classification system, portends a profound and positive impact on the classification, safeguarding, and declassification of national security information.

We are most excited about the challenges and prospects that the new security classification system creates. We are also committed to making it work as effectively as possible. Our next report will highlight our efforts in working with the agencies to bring about these changes.

Respectfully,

Steven Garfinkel

Steven Garfinkel, Director
Information Security Oversight Office

Summary of FY 1994 Program Activity

The FY 1994 Report to the President is the twelfth to examine the security classification program under E.O. 12356. The following data highlight ISOO's findings.

Classification

- The number of original classification authorities decreased by 200 to 5,461.
- Reported original classification decisions decreased by more than 40,000 to 204,683.
- Reported derivative classification decisions decreased by almost .6 million to 4,569,214.
- The total of all classification actions reported for FY 1994 decreased 26% to 4,773,897.
- DOD accounted for 57% of all classification decisions; CIA 31%; Justice 8%; State 3%; and all other agencies 1%.

Declassification

- Under the systematic review program, agencies reviewed 13,309,504 pages of historically valuable records, 47% more than in FY 1993; and declassified 11,222,780 pages, 70% more than in FY 1993.
- Agencies received 4,276 new mandatory review requests.
- Under mandatory review, agencies declassified in full 113,741 pages; declassified in part 154,389 pages; and retained classification in full on 55,815.
- Agencies received 126 new mandatory review appeals.
- On appeal, agencies declassified in whole or in part 2,668 additional pages.

Safeguarding

- Agencies conducted 12,753 self-inspections, 34% fewer than in FY 1993.
- Agencies reported 12,961 infractions, 31% fewer than in FY 1993.

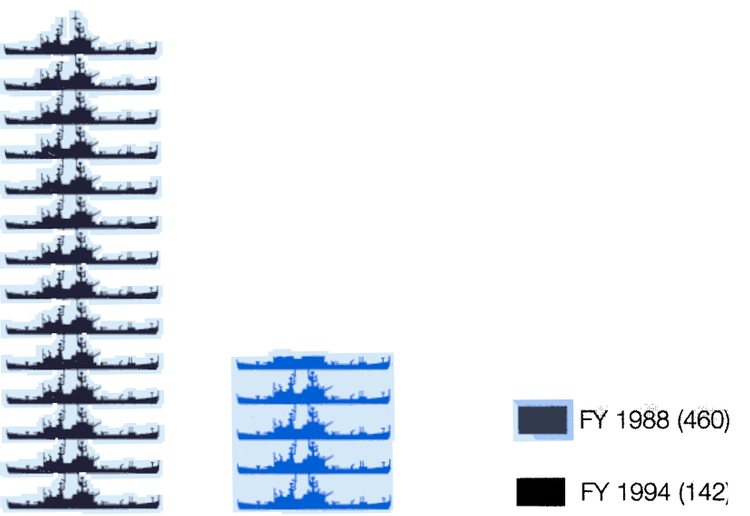
Table of Contents

A Success Story

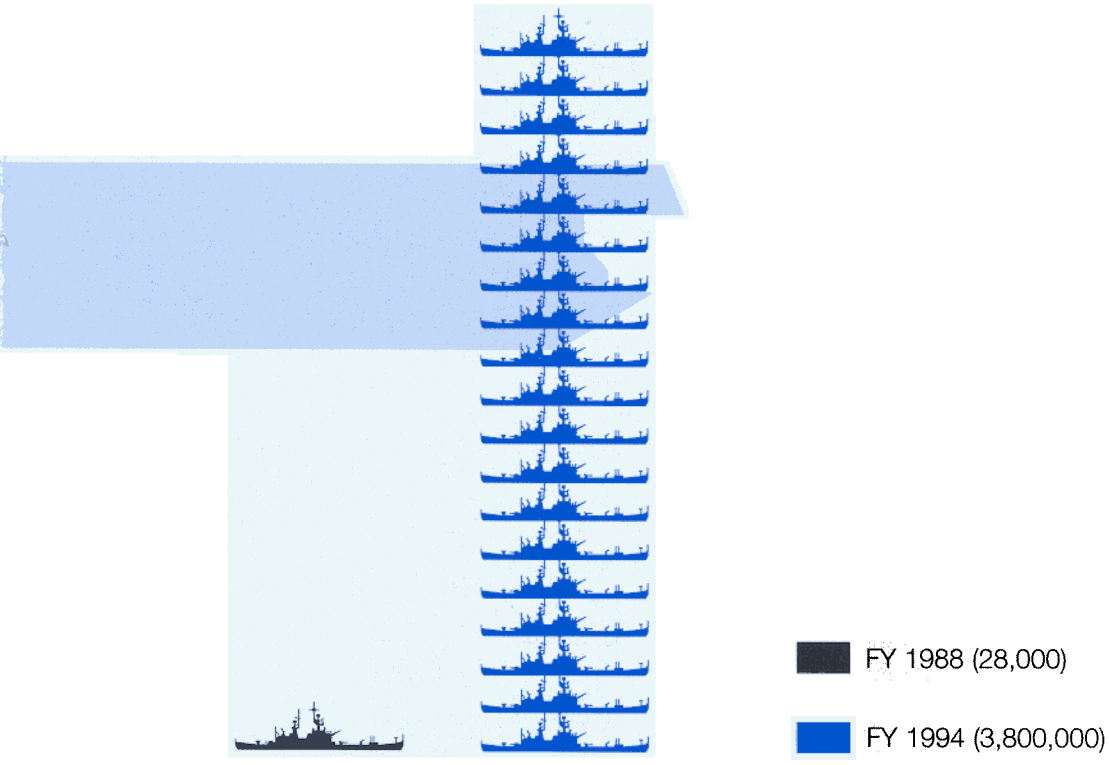
FY 1994 saw improvement in the security classification programs of many agencies. One agency in particular merits being spotlighted: the Department of the Navy. During the last seven years (1988-1994), Navy has turned the quality of its security classification and declassification programs completely around. A combination of highly competent personnel and senior management interest and involvement came together to achieve Navy's current level of success. ISOO expects this level of performance to continue with Navy's implementation of Executive Order 12958, "Classified National Security Information." Highlights of the Navy turnaround follow.

- Reduced the number of its original classification authorities from 460 in FY 1988, to 142 in FY 1994.
- Created an active systematic declassification review program that went from reviewing only 28,000 pages in FY 1988, to 3.8 million pages in FY 1994.
- Increased the percentage of reviewed pages declassified from 75% in FY 1988 to 97% in FY 1994.
- Maintained a consistent level of oversight through its inspections programs, even with downsizing.
- Maintained over 1,000 classification guides covering a variety of subjects, including war-gaming, surface operations, aircraft, and missile technology.
- Maintained an active review program of its classification guides to ensure that the data are accurate, that they are "user friendly," and that they are unclassified whenever possible.

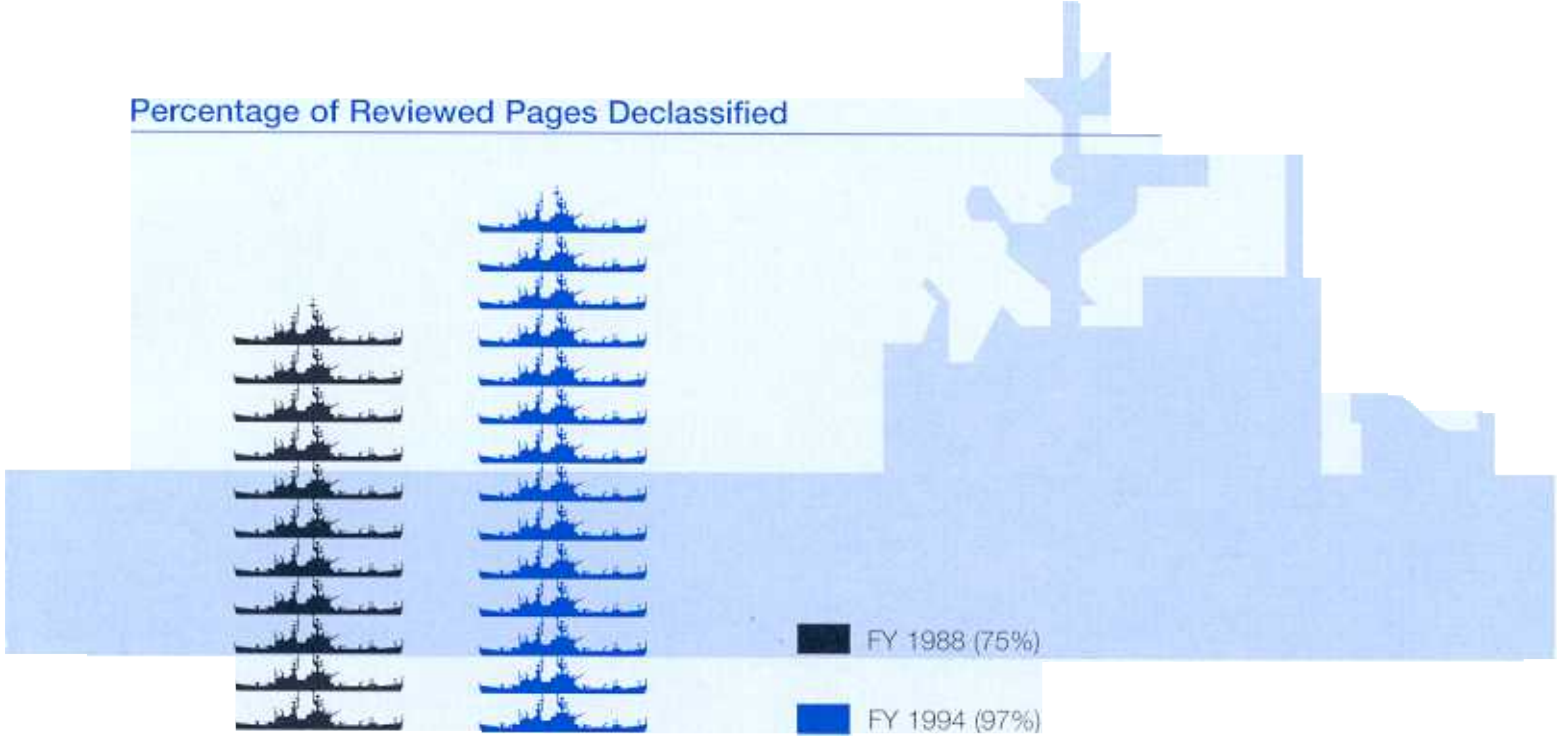
Number of Original Classification Authorities



Pages Reviewed



Percentage of Reviewed Pages Declassified



Commission on Protecting and Reducing Government Secrecy

The Foreign Relations Authorization Act for Fiscal Years 1994 and 1995 established the Commission on Protecting and Reducing Government Secrecy. Senator Daniel Patrick Moynihan chairs the twelve member, two year bipartisan panel. Representative Larry Combest serves as Vice Chairman. The other members of the Commission, listed alphabetically, include:

The Honorable John M. Deutch

The Honorable Martin C. Faga

Ms. Alison B. Fortier

The Honorable Richard K. Fox, Jr.

Representative Lee H. Hamilton

Senator Jesse Helms

Ms. Ellen Hume

Professor Samuel P. Huntington

The Honorable John D. Podesta

The Honorable Maurice Sonnenberg

The Commission's mandate is to review procedures for classifying information and make recommendations to (1) reduce the volume of information classified; and (2) improve procedures relating to the granting of security clearances.

Executive Order 12937

"Declassification of Selected Records Within the National Archives of the United States"

On November 10, 1994, President Clinton issued an Executive order that declassified, in bulk, a selection of classified records within the National Archives. This unprecedented Order declassified approximately 45 million pages or 14% of the National Archives holdings of classified material, including classified holdings through the end of World War II, and an equal number dating into the 1970s.

Executive Order 12937

THE WHITE HOUSE,
November 10, 1994

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

Section 1. The records in the National Archives of the United States referenced in the list accompanying this order are hereby declassified.

Sec. 2. The Archivist of the United States shall take such actions as are necessary to make such records available for public research no later than 30 days from the date of this Order, except to the extent that the head of an affected agency and the Archivist have determined that specific information within such records must be protected from disclosure pursuant to an authorized exemption to the Freedom of Information Act, 5 U.S.C. 552, other than the exemption that pertains to national security information.

Sec. 3. 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.

Records in the following record groups ("RG") in the National Archives of the United States shall be declassified. Page numbers are approximate. A complete list of the selected records is available from the Archivist of the United States.

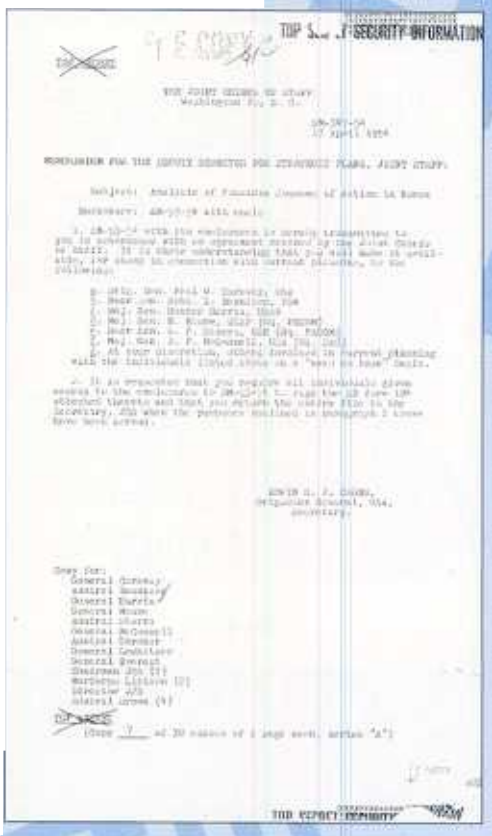
I. All unreviewed World War II and earlier records, including:

A. RG 18, Army Air Forces	1,722,400 pp.
B. RG 65, Federal Bureau of Investigation	362,500 pp.
C. RG 127, United States Marine Corps	195,000 pp.
D. RG 216, Office of Censorship	112,500 pp.
E. RG 226, Office of Strategic Services	415,000 pp.
F. RG 60, United States Occupation Headquarters	4,422,500 pp.
G. RG 331, Allied Operational and Occupation Headquarters, World War II (including 350 reels of Allied Force Headquarters)	3,097,500 pp.

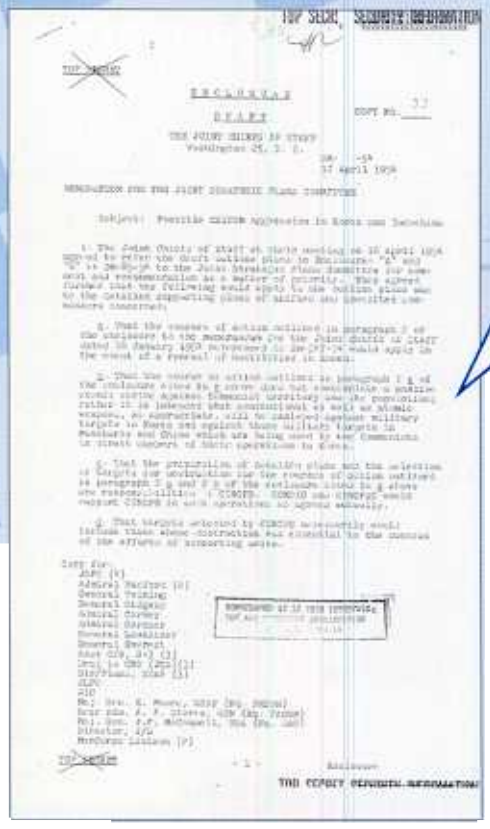
H. RG 332, United States Theaters of War, World War II	1,182,500 pp.
I. RG 338, Mediterranean Theater of Operations and European Command	9,500,000 pp.
Subtotal for World War II and earlier	21 million pp.

II. Post-1945 Collections *(Military and Civil)*

A. RG 19, Bureau of Ships, Pre-1950 General Correspondence (selected records)	1,732,500 pp.
B. RG 51, Bureau of the Budget, 52.12 Budget Preparation Branch, 1952-1969	142,500 pp.
C. RG 72, Bureau of Aeronautics (Navy) (selected records)	5,655,000 pp.
D. RG 166, Foreign Agricultural Service, Narrative Reports, 1955-61	1,272,500 pp.
E. RG 313, Naval Operating Forces (selected records)	407,500 pp.
F. RG 319, Office of the Chief of Military History Manuscripts and Background Papers (selected records)	933,000 pp.
G. RG 337, Headquarters, Army Ground Forces (selected records)	1,269,700 pp.
H. RG 341, Headquarters, United States Air Force (selected records)	4,870,000 pp.
I. RG 389, Office of the Provost Marshal General (selected records)	448,000 pp.
J. RG 391, United States Army Regular Army Mobil Units	240,000 pp.
K. RG 428, General Records of the Department of the Navy (selected records)	31,250 pp.
L. RG 472, Army Vietnam Collection (selected records)	5,864,000 pp.
Subtotal for Other	22.9 million pp.
TOTAL	**43.9 million pp.**



The Joint Chiefs of Staff
Washington 25, D.C.
Memorandum for the
Joint Strategic Plans Committee
17 April 1954



b. the course of action outlined in paragraph 2 a of the enclosure cited in a above does not contemplate a massive atomic strike against Communist territory and its population . . . .

Now declassified budget response from NASA titled "Manned Lunar Landing Program-Status and Prospects"

CONFIDENTIAL

Manned Lunar Landing Program - Status and Prospects

Before discussing the status and prospects of the manned lunar landing program, it is important to place the lunar landing objective in its proper perspective. Our early national space endeavors were scrutinized severely to what we had or could improvise, primarily by adaptation of existing military rocket technology. At the same time, we began other efforts intended to extend and expand our capability.

The lunar landing goal was selected not only because it provided an explicit response to the Soviet challenge but also because, in its achievement, we would achieve important overarching program accomplishments and create basic national resources needed for a variety of purposes -- scientific and engineering information, hardware, facilities, trained manpower, and astronautic and operational skills and experience. The lunar landing goal also provided two other prerequisites for these efforts. No later evidence has developed to indicate that commitment to the lunar landing goal was unsound.

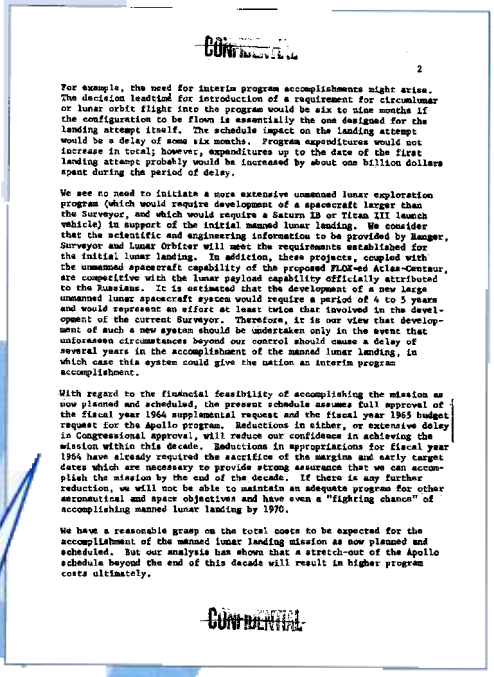
Similarly, no evidence has developed which invalidates the basic feasibility of accomplishing the mission as now planned and scheduled.

There are no known technical problems which should prevent accomplishment of manned lunar landing within this decade, as planned. The mission is technically feasible within this time frame because we begin new projects or engineering approaches not foreseen to be required. Unknown technical problems, which would delay the schedule, are believed to be primarily those which might arise if the characteristics of the lunar surface prove to be greatly different from our current estimates. Other technical factors, such as space radiation, micrometeoroid environment and equipment development, are not expected to affect materially the technical feasibility of mission accomplishment, provided the necessary funding is made available on a timely basis.

The present program plan provides the capability to capitalize on early successes in the test program as well as the depth which is deemed necessary to provide a reasonable assurance of mission accomplishment. Completion of qualification of the Saturn V launch vehicle and the Apollo spacecraft as presently planned by the eighth flight of the Saturn V, if that objective is met, the ninth Saturn V flight would provide for the earliest initial lunar landing attempt. If these objectives are not met as planned, up to six additional Saturn V flights remain available for accomplishment of the initial lunar landing.

The present program of fifteen Saturn V flights could also accompass one or two circumlunar or lunar orbit flights if such should become necessary or desirable. The present planning does not call for a circumlunar mission, since Surveyor and Lunar Orbiter are designed to provide necessary data on the lunar surface characteristics. However, we recognize the possibility that there may be compelling reasons for a manned circumlunar or lunar orbit flight prior to the initial landing attempt.

CONFIDENTIAL



CONFIDENTIAL

2

For example, the need for interim program accomplishments might arise. The decision leadtime for introduction of a requirement for circumlunar or lunar orbit flight into the program would be six to nine months if the configuration to be flown is essentially the one designed for the landing attempt itself. The schedule impact on the landing attempt would be a delay of some six months. Program expenditures would not increase in total; however, expenditures up to the date of the first landing attempt probably would be increased by about one billion dollars spent during the period of delay.

We see no need to initiate a more extensive unmanned lunar exploration program (which would require development of a spacecraft larger than the Surveyor, and which would require a Saturn IB or Titan III launch vehicle) in support of the initial manned lunar landing. We consider that the scientific and engineering information to be provided by Ranger, Surveyor and Lunar Orbiter will meet the requirements established for the initial lunar landing. In addition, these projects, coupled with the unmanned spacecraft capability of the proposed FLOX-ed Atlas-Centaur, are competitive with the lunar payload capability officially attributed to the Russians. It is estimated that the development of a new large unmanned lunar spacecraft system would require a period of 4 to 5 years and would represent an effort at least twice that involved in the development of the current Surveyor. Therefore, it is our view that development of such a new system should be undertaken only in the event that unforeseen circumstances beyond our control should cause a delay of several years in the accomplishment of the manned lunar landing, in which case this system could give the nation an interim program accomplishment.

With regard to the financial feasibility of accomplishing the mission as now planned and scheduled, the present schedule assumes full approval of the fiscal year 1966 supplemental request and the fiscal year 1965 budget request for the Apollo program. Reductions in either, or extensive delay in Congressional approval, will reduce our confidence in achieving the mission within this decade. Reductions in appropriations for fiscal year 1966 have already required the sacrifice of the margins and early target dates which are necessary to provide strong assurance that we can accomplish the mission by the end of the decade. If there is any further reduction, we will not be able to maintain an adequate program for other aeronautical and space objectives and have even a "fighting chance" of accomplishing manned lunar landing by 1970.

We have a reasonable grasp on the total costs to be expected for the accomplishment of the manned lunar landing mission as now planned and scheduled. But our analysis has shown that a stretch-out of the Apollo schedule beyond the end of this decade will result in higher program costs ultimately.

CONFIDENTIAL

> Reductions in [the 1965 budget] will reduce our confidence in achieving [a lunar landing] within this decade.

Cover for now declassified Army report titled "The Role of Cambodia in the NVN-VC War Effort 1964-1970" 13 April 1971

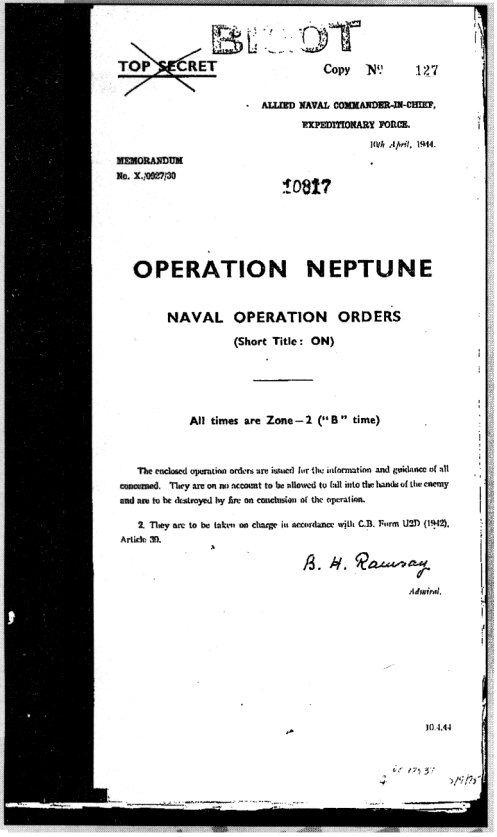
TOP SECRET
NO FOREIGN DISSEM

THE ROLE OF CAMBODIA
IN THE
NVN-VC WAR EFFORT
1964-1970
OVERVIEW

OFFICE OF THE
ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
DEPARTMENT OF THE ARMY

TOP SECRET

Allied Naval Commander-in-Chief
Expeditionary Force
Naval Operation Orders
10 April 1944



TOP SECRET

Copy No. 127

ALLIED NAVAL COMMANDER-IN-CHIEF,
EXPEDITIONARY FORCE.

10th April, 1944.

MEMORANDUM
No. X./0927/30

10817

OPERATION NEPTUNE

NAVAL OPERATION ORDERS

(Short Title: ON)

All times are Zone—2 ("B" time)

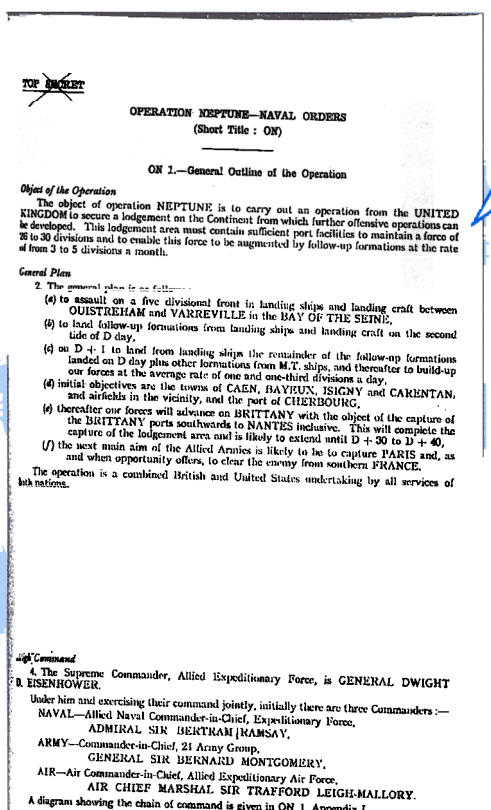
The enclosed operation orders are issued for the information and guidance of all concerned. They are on no account to be allowed to fall into the hands of the enemy and are to be destroyed by fire on conclusion of the operation.

2. They are to be taken on charge in accordance with C.B. Form 0217 (1942), Article 30.

B. H. Ramsay

Admiral.

10.4.44



TOP SECRET

OPERATION NEPTUNE—NAVAL ORDERS
(Short Title: ON)

ON 1.—General Outline of the Operation

Object of the Operation

The object of operation NEPTUNE is to carry out an operation from the UNITED KINGDOM to secure a lodgement on the Continent from which further offensive operations can be developed. This lodgement area must contain sufficient port facilities to maintain a force of 26 to 30 divisions and to enable this force to be augmented by follow-up formations at the rate of from 3 to 5 divisions a month.

General Plan

2. The general plan is as follows:—

(a) to assault on a five divisional front in landing ships and landing craft between OUISTREHAM and VARREVILLE in the BAY OF THE SEINE,

(b) to land follow-up formations from landing ships and landing craft on the second tide of D day,

(c) on D + 1 to land from landing ships the remainder of the follow-up formations landed on D day plus other formations from M.T. ships, and thereafter to build-up our forces at the average rate of one and one-third divisions a day,

(d) initial objectives are the towns of CAEN, BAYEUX, ISIGNY and CARENTAN, and airfields in the vicinity, and the port of CHERBOURG,

(e) thereafter our forces will advance on BRITTANY with the object of the capture of the BRITTANY ports southwards to NANTES inclusive. This will complete the capture of the lodgement area and is likely to extend until D + 30 to D + 40,

(f) the next main aim of the Allied Armies is likely to be to capture PARIS and, as and when opportunity offers, to clear the enemy from southern FRANCE.

The operation is a combined British and United States undertaking by all services of both nations.

...ief Command

4. The Supreme Commander, Allied Expeditionary Force, is GENERAL DWIGHT D. EISENHOWER.

Under him and exercising their command jointly, initially there are three Commanders:—

NAVAL—Allied Naval Commander-in-Chief, Expeditionary Force,
ADMIRAL SIR BERTRAM RAMSAY.

ARMY—Commander-in-Chief, 21 Army Group,
GENERAL SIR BERNARD MONTGOMERY.

AIR—Air Commander-in-Chief, Allied Expeditionary Air Force,
AIR CHIEF MARSHAL SIR TRAFFORD LEIGH-MALLORY.

A diagram showing the chain of command is given in ON 1, Appendix I.

Principles of Naval Command

The object of operation NEPTUNE is to carry out an operation from the UNITED KINGDOM to secure a lodgement on the Continent . . . .

Executive Order 12951

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

On February 22, 1995, President Clinton issued an Executive order that, for the first time, will result in the declassification and public availability of historical intelligence imagery.

Executive Order 12951

THE WHITE HOUSE,
February 22, 1995

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.

Sec. 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.

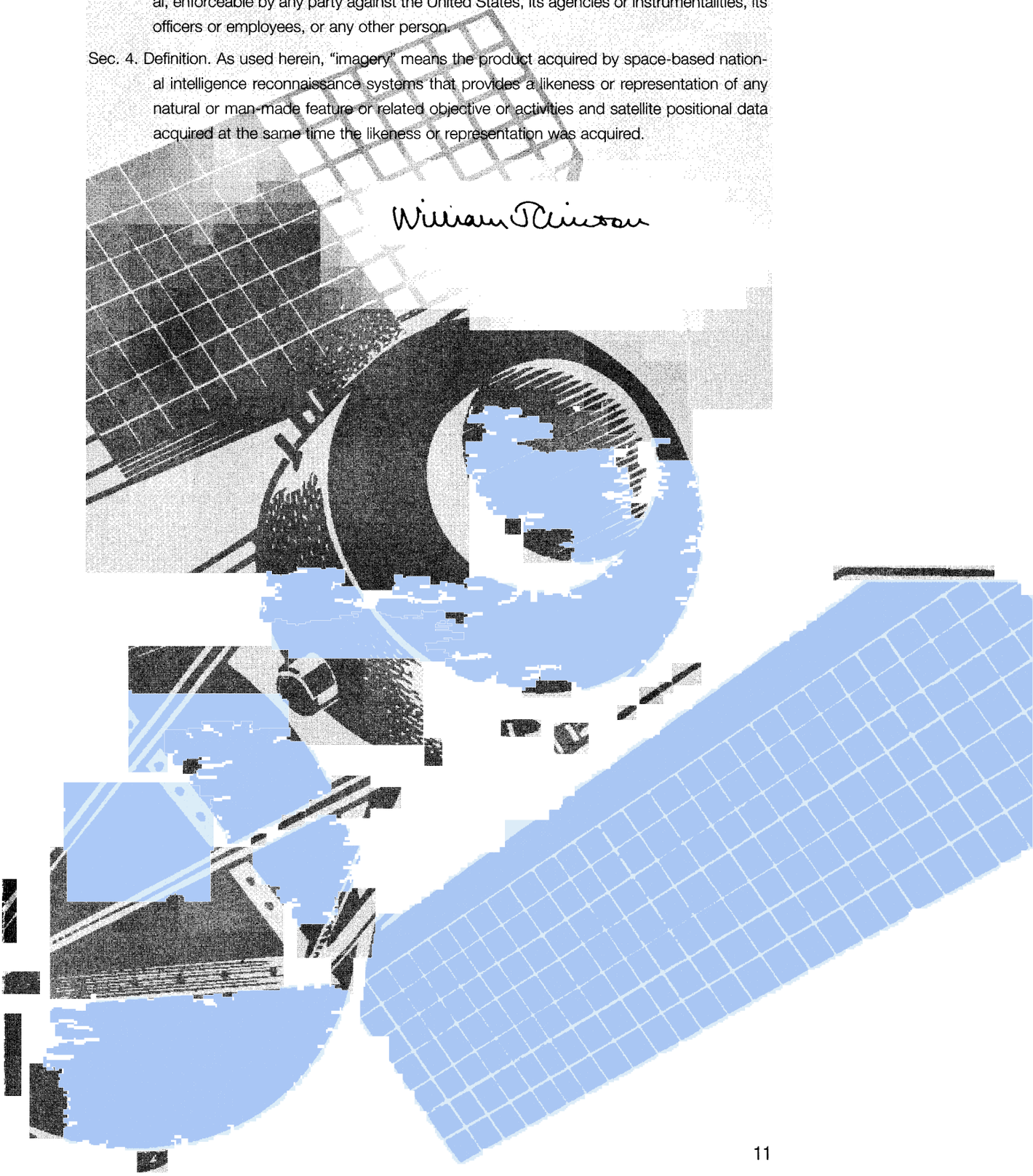
Sec. 3. General Provisions.

(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.

Sec. 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



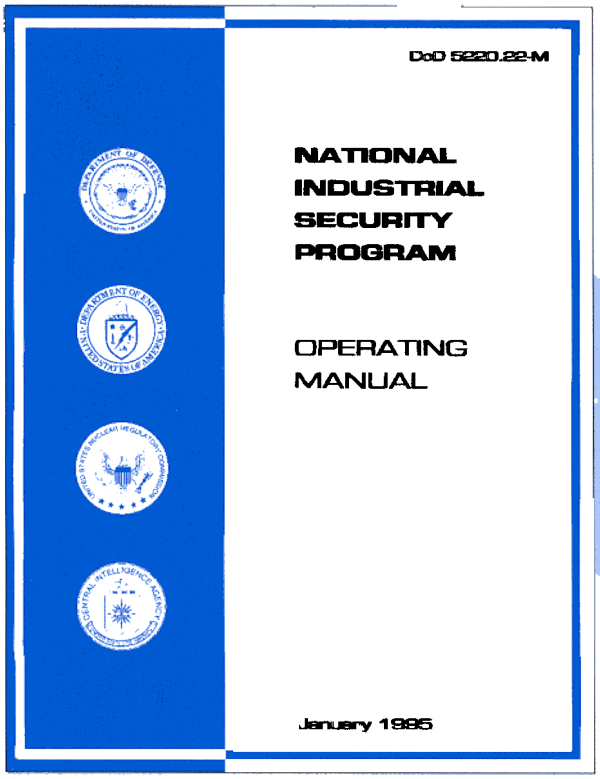
Major step toward full implementation of the National Industrial Security Program

On October 5, 1994, then Deputy Secretary of Defense John Deutch, acting as the Executive Agent, announced the release of the National Industrial Security Program Operating Manual (NISPOM). The product of several years of effort by Government and industry security professionals, the NISPOM is the centerpiece of the National Industrial Security Program (NISP) established by Executive Order 12829, "National Industrial Security Program," issued in 1993. The issuance of the Manual should mark the beginning of full implementation of the NISP.

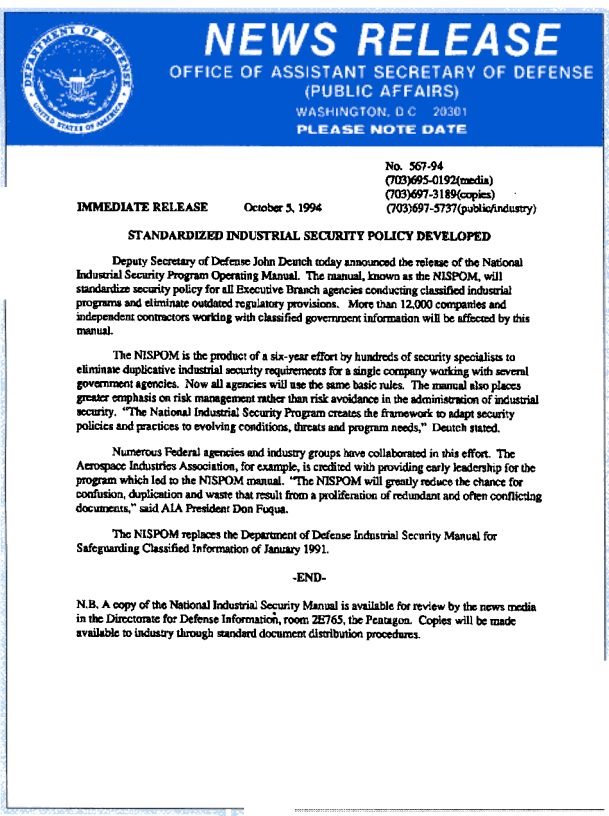
The rationale for the establishment of the NISP was the desire to standardize security procedures for protecting classified information held by industry. Its aim is to provide for a "single, integrated, cohesive" industrial security program by replacing conflicting, overlapping and unnecessary requirements with uniform standards. The NISPOM gives this aim operational expression. Consequently, the initial test of the effectiveness of the NISPOM is whether it achieves the fundamental purposes of E.O. 12829. The ISOO is presently reviewing the NISPOM for this purpose. The review is not yet completed. Still, some brief comments are pertinent at this juncture.

The NISPOM generally succeeds in providing a logical progression through sections on classification, markings, declassification, safeguarding and other topics. However, some unresolved issues linger and will require a strong commitment on the part of the agencies involved to resolve them. Also, a significant number of contractors have expressed concern about conflicting and confusing guidance on implementation of the program; lack of clarity of some of the provisions of the NISPOM; and considerable delays in its availability. Some of these concerns were raised by industry representatives at the April 1995 meeting of the National Industrial Security Program Policy Advisory Committee (NISPPAC). The NISPPAC, which consists of representatives from both Government and industry, advises the ISOO Director on all matters concerning the program, including recommending changes in policy and proposing solutions to issues in dispute.

The issuance of the NISPOM holds potential for meeting the goals of E.O. 12829. As a major change in the way of doing business, no one should be surprised that there have been some problems following its issuance. What is needed at this time are renewed efforts to continue progress toward a single, integrated industrial security program. For this purpose, agencies should give a strong and fresh emphasis to setting aside parochial interests and demonstrating commitment to achieve the goals of the National Industrial Security Program.



Cover of the National Industrial Security Program Operating Manual.



NEWS RELEASE

OFFICE OF ASSISTANT SECRETARY OF DEFENSE
(PUBLIC AFFAIRS)
WASHINGTON, D.C. 20301
PLEASE NOTE DATE

No. 567-94
(703)695-0192(media)
(703)697-3189(copies)
(703)697-5737(public/industry)

IMMEDIATE RELEASE October 5, 1994

STANDARDIZED INDUSTRIAL SECURITY POLICY DEVELOPED

Deputy Secretary of Defense John Deutch today announced the release of the National Industrial Security Program Operating Manual. The manual, known as the NISPOM, will standardize security policy for all Executive Branch agencies conducting classified industrial programs and eliminate outdated regulatory provisions. More than 12,000 companies and independent contractors working with classified government information will be affected by this manual.

The NISPOM is the product of a six-year effort by hundreds of security specialists to eliminate duplicative industrial security requirements for a single company working with several government agencies. Now all agencies will use the same basic rules. The manual also places greater emphasis on risk management rather than risk avoidance in the administration of industrial security. "The National Industrial Security Program creates the framework to adapt security policies and practices to evolving conditions, threats and program needs," Deutch stated.

Numerous Federal agencies and industry groups have collaborated in this effort. The Aerospace Industries Association, for example, is credited with providing early leadership for the program which led to the NISPOM manual. "The NISPOM will greatly reduce the chance for confusion, duplication and waste that result from a proliferation of redundant and often conflicting documents," said AIA President Don Fuqua.

The NISPOM replaces the Department of Defense Industrial Security Manual for Safeguarding Classified Information of January 1991.

-END-

N.B. A copy of the National Industrial Security Manual is available for review by the news media in the Directorate for Defense Information, room 2E765, the Pentagon. Copies will be made available to industry through standard document distribution procedures.

October 1994 press release announcing the release of the National Industrial Security Program Operating Manual.

Classification

Original Classifiers

Original classification authorities, also called original classifiers, are those individuals designated in writing, either by the President or by selected agency heads, to classify information in the first instance. Under E.O. 12356, only original classifiers determine what information, if disclosed without authority, could reasonably be expected to cause damage to the national security.

For FY 1994, the number of original classifiers throughout the executive branch was 5,461, exactly 200 fewer than last year. This figure, for the fourth consecutive year, represents the lowest number of original classifiers ever reported by ISOO. ISOO attributes the decrease in the number of original classifiers over the past several years primarily to the end of the Cold War and the on-going efforts to downsize Government. Since disparities exist among agencies with comparable original classification authority, ISOO believes further reductions are possible without having a negative impact on agency operations. The issuance of Executive Order 12958, "Classified National Security Information," offers an excellent opportunity to achieve further reductions. Agency heads and senior agency officials will be reviewing each and every one of the individuals with original classification authority before redelegating authority under the new Executive order. Therefore, ISOO will continue to encourage agencies to use this occasion to limit the number of original classification authorities to the lowest level possible.

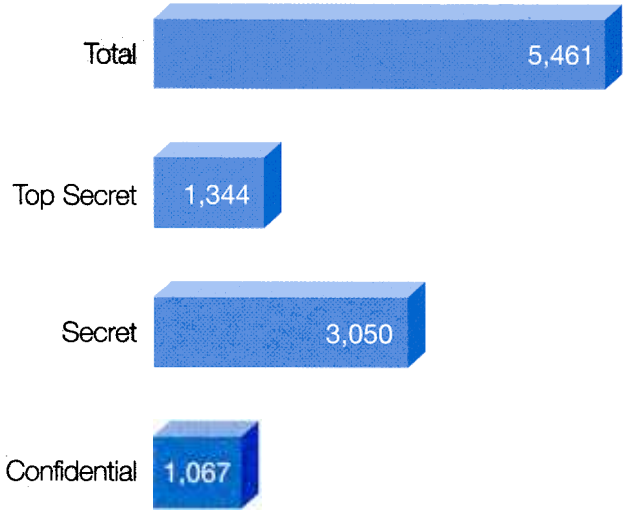
In FY 1994, agencies reported decreases in the number of original classifiers for all three levels. At the **Top Secret** and **Confidential** levels, agencies reported decreases of 1%, while the number of **Secret** original classifiers decreased by an impressive 5%. ISOO wishes to recognize several agencies for their efforts to reduce the number of original classifiers. In particular, ISOO applauds AID and FEMA for reporting decreases of 84% and 73%, respectively. Also reporting significant reductions were DOE, Treasury and DOD, which has been at the forefront in reducing its number of original classifiers for the past several years. Please refer to "A Success Story" on the Navy's progress in this and other areas in recent years.

umber of

al classifiers

nues to fall

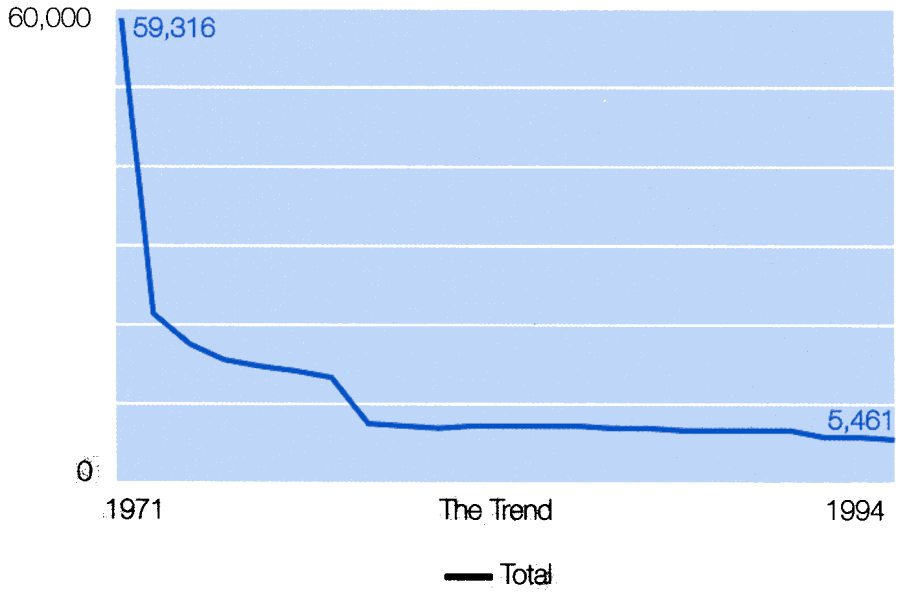
Original Classifiers FY 1994



Secret level classifie

decrease by 5%

one year

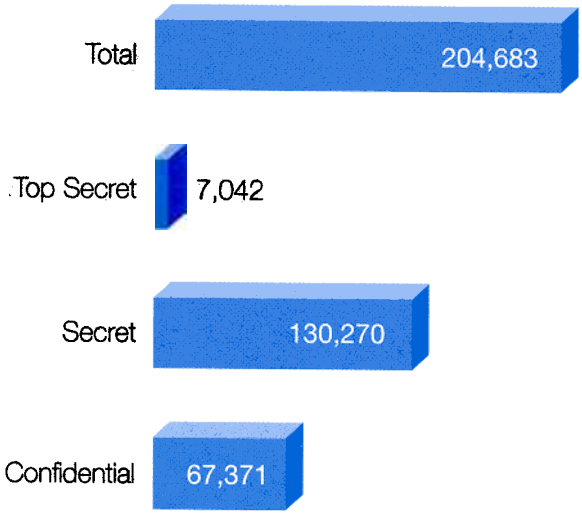


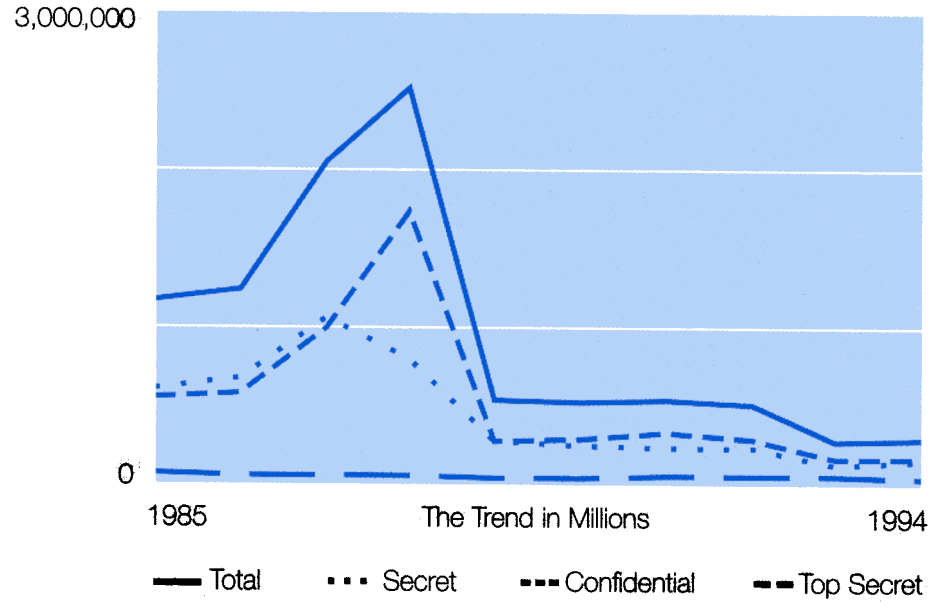
Original Classification

Original Classification is an initial determination by an authorized classifier that information requires extraordinary protection, because unauthorized disclosure of the information could reasonably be expected to cause damage to the national security. The process of original classification ordinarily includes both the determination of the need to protect the information and the placement of markings to identify the information as classified. By definition, original classification precedes all other aspects of the security classification system, e.g., derivative classification, safeguarding and declassification. Therefore, ISOO often refers to the number of original classification actions as the most important figure that it reports.

Overall original classification down by 17%; Top Secret decisions by 61%

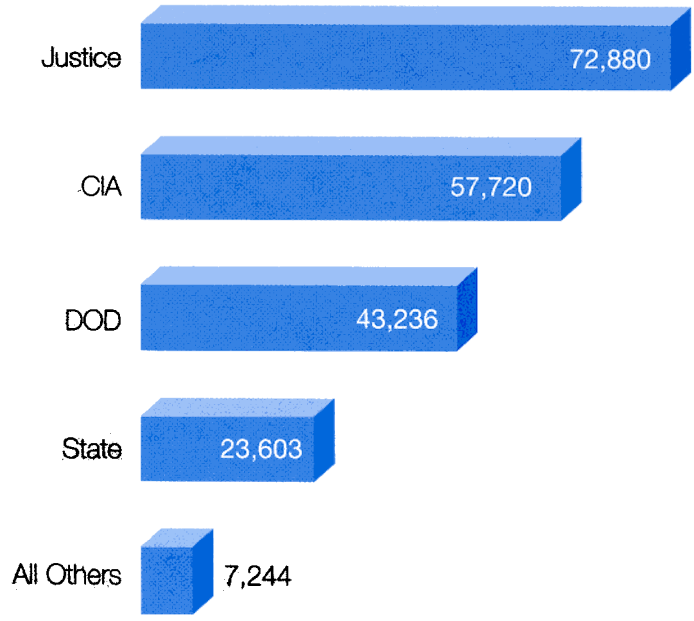
Original Activity FY 1994





For FY 1994, agencies reported a total of 204,683 original classification decisions. This figure represents a decrease of 17% over the number of original classification decisions reported in FY 1993, and is the lowest number of original classification actions ever reported by ISOO. Again, ISOO believes the decrease in the number of original classification decisions over the past several years is a result of on-going efforts to downsize Government and the end of Cold War tensions. By classification level, both **Top Secret** and **Confidential** decisions decreased significantly by 61% and 31%, respectively, while the number of **Secret** original classification actions remained relatively unchanged. The decrease in **Top Secret** decisions is most impressive since it reduces the number of classifications that are, by far, the most costly to maintain.

Original Activity By Agency FY 1994



Four agencies, Justice, CIA, DOD, and State, continue to account for almost 97% of all original classification decisions. Of these agencies, Justice reported the highest number, with a total of 72,880 original classification decisions. However, this number represents a decrease of 8% in original classification decisions at Justice from the figure reported in FY 1993. CIA reported a total of 57,720 original classification decisions, which represent an increase of 15% from the prior year. CIA attributes this increase to the agency's reorganization of personnel, which resulted in a modification to the agency's sampling method. ISOO believes the increase is not a matter of serious concern but intends to monitor the situation closely. ISOO applauds DOD for reducing its number of original classification actions by an impressive 47%. State also reported a decrease of 13% in the number of original classification decisions.

DOD reduce

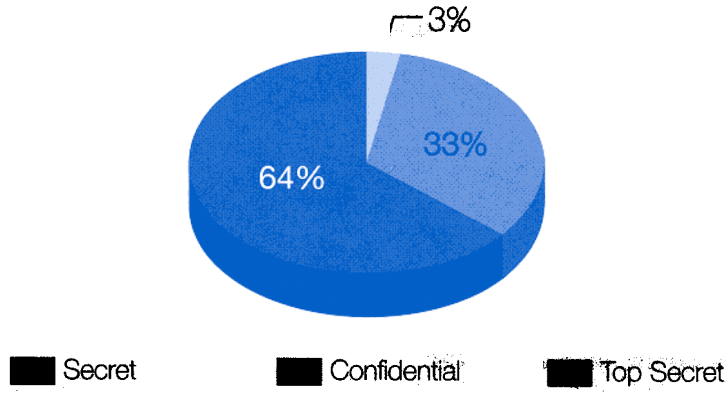
original classifica

activity by 47%

For the agencies with smaller programs, the data collected show a decrease of 12% in the number of original classification decisions. In particular, ISOO commends NASA, Treasury, and Commerce, which reported decreases of 80%, 31%, and 25%, respectively, in the number of original classification actions.

As part of the original classification process, the classifier must determine a time frame for the protection of the information. This is commonly called "duration" of classification. E.O. 12356 provides classifiers with two means of designating the duration of classification for national security information, better known as declassification instructions. First, the information may be marked for declassification upon a specific date or event. For example, a classifier may determine that the information's sensitivity will lapse upon the completion of a particular project. The event would be noted on the face of the document, and when the project had

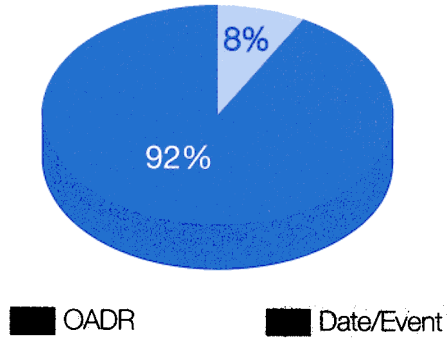
Original Classification Levels FY 1994



been completed, the information would automatically be declassified. Only if a specific date or event cannot be determined at the time of classification is the classifier authorized to use the second means, marking the document with the notation "Originating Agency's Determination Required" ("OADR"). "OADR" indicates that the information must be reviewed by the originating agency before declassification action may be taken.

Duration of Classification FY 1994

E.O. 12958 will eliminate the indefinite duration of classification



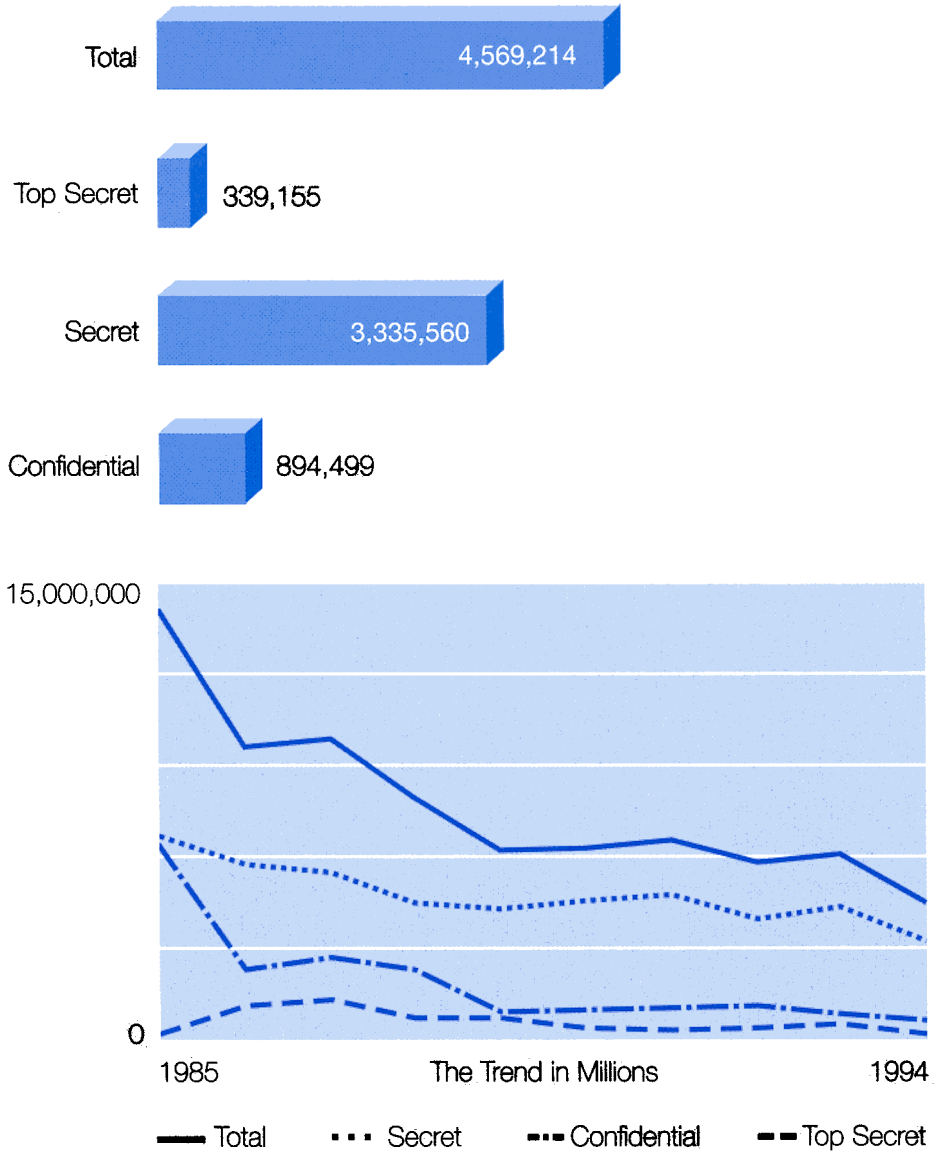
For FY 1994, 8% of all original classification decisions were marked for declassification with a specific date or event, as compared to 3% of all original classification actions reported in FY 1993. Although this represents a very positive improvement, ISOO believes both proportions are too low. Executive Order 12958, "Classified National Security Information," which becomes effective on October 14, 1995, includes provisions specifically designed to address the problem of indefinite classification, including the elimination of the "OADR" provision.

Derivative Classification

Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form classified source information. Information may be derivatively classified in two ways: (a) through the use of a source document, usually correspondence or publications by an original classification

authority; or (b) through the use of a classification guide. A classification guide is a set of instructions issued by an original classification authority. It pertains to a particular subject and describes the elements of information about that subject that must be classified, and the level and duration of classification. Only executive branch or Government contractor employees with the appropriate security clearance, who are required by their work to restate classified source information, may classify derivatively.

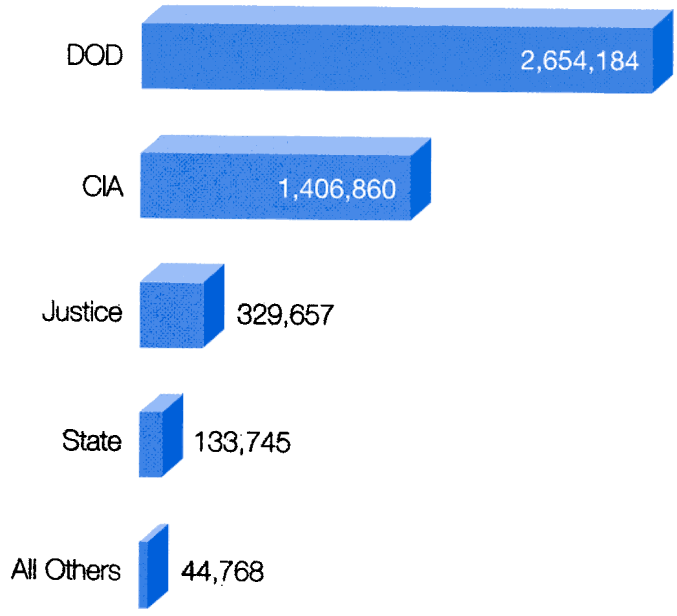
Derivative Activity FY 1994



In ten years derivative decision have decreased by more than two-thirds

Derivative classification decreases by almost 1.6 million actions

Derivative Activity By Agency FY 1994



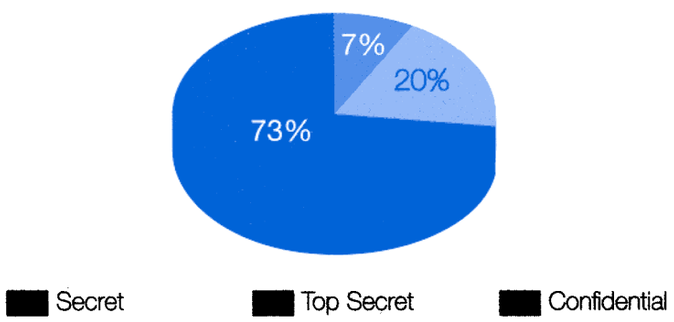
For FY 1994, agencies reported 4,569,214 derivative classification actions. This figure represents a significant decrease of almost 26% from that reported in FY 1993, and is the lowest number ever reported by ISOO. Again, ISOO attributes this decrease to the continuing efforts to downsize Government programs, operations, and personnel and the absence of any major international conflict involving the United States. During FY 1994, the four major classifying agencies reported significant reductions in the number of derivative classification actions. Among these agencies, Justice led the way, reporting a 56% reduction in derivative classification actions. DOD reported a 28% reduction, State reported a 13% reduction, and CIA reported an 8% reduction in the number of derivative classification actions from FY 1993. ISOO applauds Justice, CIA, DOD, and State for their efforts in reducing significantly the number of derivative classification actions.

All other agencies reported 44,768 derivative classification actions, a 20% reduction from the prior year. Among these agencies, ISOO commends the following agencies for reducing the number of derivative classification actions for FY 1994: AID (34%), DOT (28%), ITC (40%), OPIC (67%), Treasury (15%), and USTR (94%).

As in the past, the breakdown of derivative classification actions by classification level differs somewhat from the breakdown of original classification decisions: **Secret** and **Top Secret** decisions continue to comprise higher percentages of the total. With respect to the proportion of **Top Secret** actions, this results from a very few activities that produce a relatively large quantity of derivative documents from classification guidance. Generally, this **Top Secret** information is highly localized, so that the percentage of **Top Secret** actions within almost all

collections of classified information is much smaller. Nevertheless, if it continues, the significant reduction in **Top Secret** derivative actions that took place in FY 1994 will have a significant long-term impact in reducing the costs of classification.

Derivative Classification Levels FY 1994



Top Secret

derivative acti

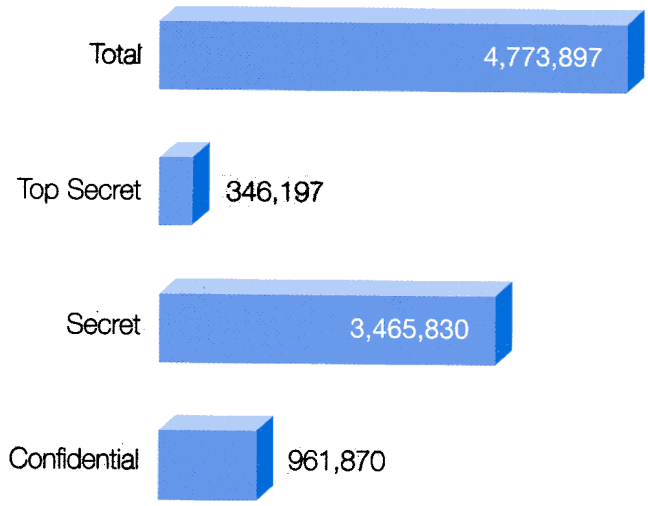
reduced by

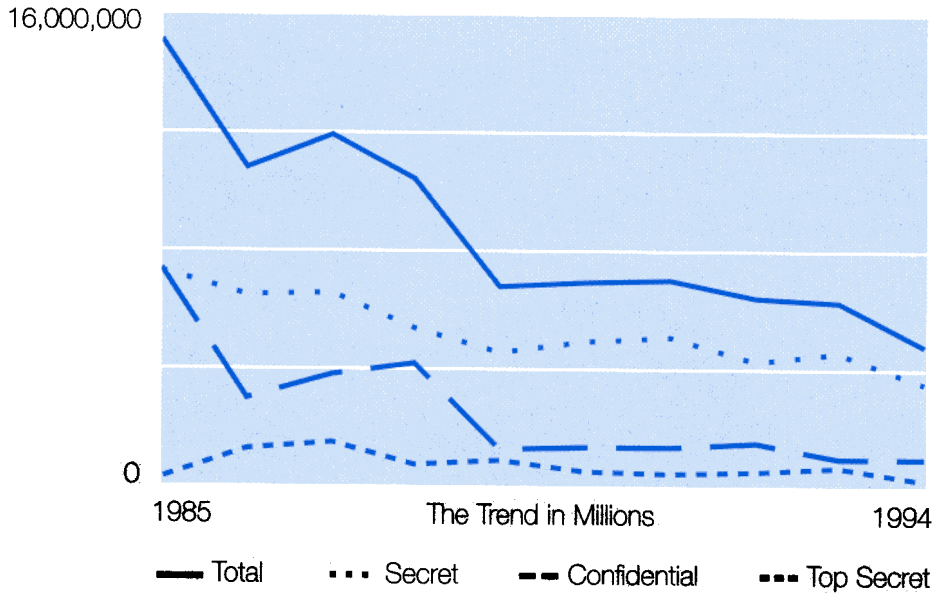
than half

Combined Classification FY 1994

By adding original and derivative classification decisions, ISOO arrives at what it calls combined classification activity. In FY 1994, combined classification activity significantly decreased by 1,634,791 (26%) to a total of 4,773,897 actions. Since derivative actions outnumbered original actions by a ratio of more than 22:1, they had a much greater impact on combined classification activity. Again, both derivative and original classification activity reached all time reported lows in FY 1994. This resulted in an all time reported low for combined classification activity.

Combined Activity FY 1994

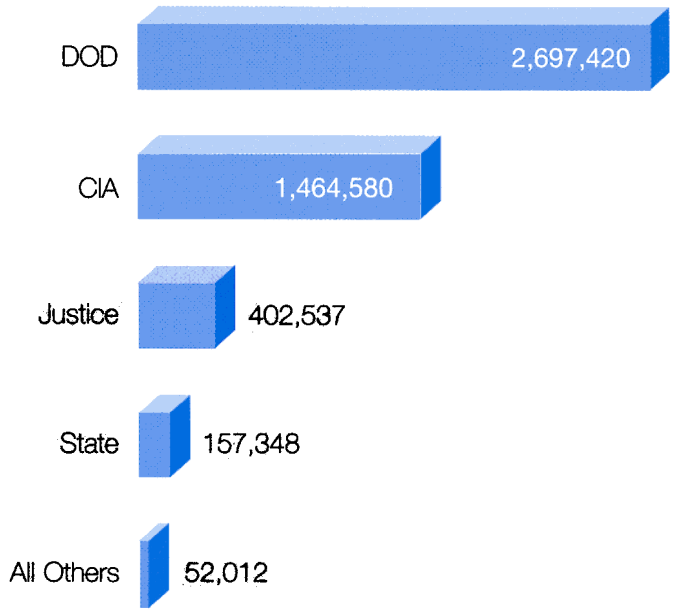




Total classification activity down 26% from last year

DOD accounted for 57% of all classification activity reported for FY 1994, CIA accounted for 31% of the total, Justice 8% and State 3%. Again, the remaining agencies accounted for only 1% of the combined classification activity. These agencies run the gamut, however, in the degree of their involvement with classified information. They range from very large departments that possess very little classified information, and generate almost none, to very small entities that exist almost exclusively in a classified environment.

Combined Activity By Agency FY 1994

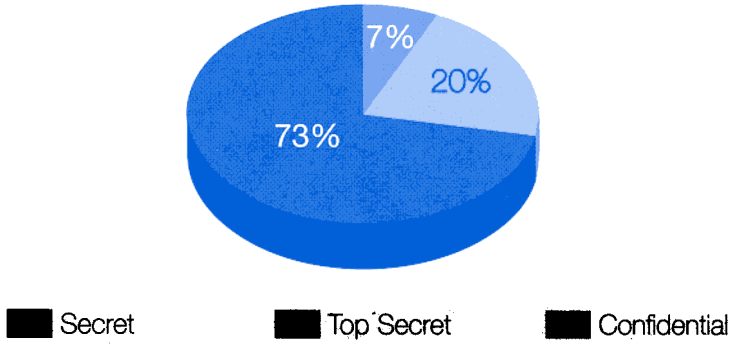


Derivative classificati

outnumbers origina

classification 22 to

Combined Classification Levels FY 1994



Declassification

0% increase

ges declassified

der systematic

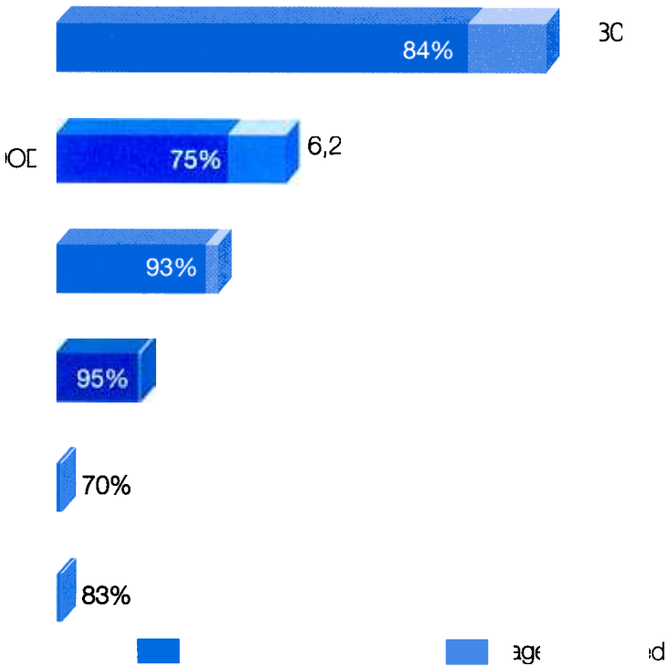
review

Systematic Review

Started in 1972, "systematic review for declassification" is the program under which classified, permanently valuable (archival) records are reviewed for purposes of declassification after the records reach a specific age. Under E.O. 12356, NARA is the only agency required to conduct a systematic review of its classified holdings. NARA ordinarily reviews its classified holdings as they become 30 years old, except for certain intelligence or cryptologic file series, which are to be reviewed as they become 50 years old. While other agencies are not required to establish a systematic review program, ISOO encourages them to do so. With the approval of the originator, agencies, including NARA, may conduct a systematic review of records that are less than 30 years old.

ISOO is pleased to report that during FY 1994, the product of the systematic review program showed its first significant increase since FY 1990. Agencies reviewed 13.3 million pages in FY 1994. This is an increase of 4.3 million pages (+47%) from FY 1993. Of the pages reviewed, 84% were declassified, a significant increase from the 73% rate reported in FY 1993. As a result of the greater number of pages reviewed and the higher declassification rate, over 11.2 million pages were declassified under the systematic review program in FY 1994. When added to the number of pages declassified under the Executive Order 12937, "Declassification of Selected Records Within the National Archives of the United States," 1994 was a banner year for declassification. With the advent of the declassification reforms in Executive Order 12958, "Classified National Security Information," these numbers should be a prelude to the future of declassification.

Systematic Review Actions By Agency FY 1994



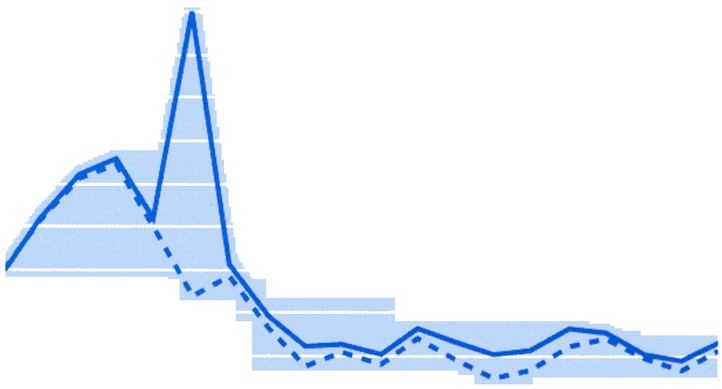
Systematic revi

and E.O. 12937

declassified more

5 million pages

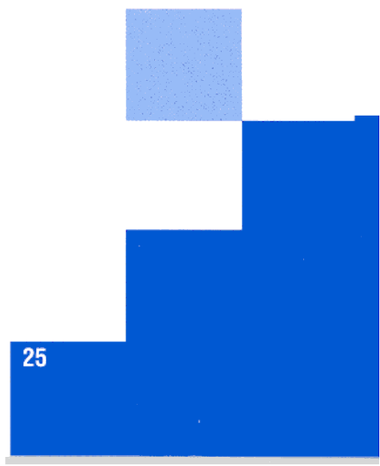
1994



The Trend in

Page Reviewe
(1994: 3.3 milli

Pages
(1994:



Although the efforts of several agencies contributed to the increase, DOD and State account for much of the program's substantial improvement. DOD accounted for the highest volume of pages reviewed in FY 1994. DOD reviewed over 6 million pages, 3 million more than in FY 1993 (+109%). While several DOD components contributed to DOD's outstanding performance, the three military services account for most of DOD's systematic review activity. Particularly noteworthy is Navy's contribution. During FY 1994, Navy reviewed 3.8 million pages, 3.2 million more than in FY 1993, almost a seven fold increase. Of the 3.8 million reviewed, Navy declassified 3.7 million pages.

DOD and State account for the large increase in declassification

State accounted for the second highest volume of pages reviewed in FY 1994. State reviewed 4.4 million pages, nearly a 3 million page increase from FY 1993. Of the 4.4 million pages reviewed, State declassified 4 million pages.

In FY 1994, the number of pages NARA reviewed decreased from 3,005,456 to 2,320,531 (-23%), with a declassification rate of 95%, a slight increase. NARA's primary explanation for the decline in its systematic review activity was a reduction in resources to conduct systematic review. For the past two years, NARA has reported that special projects, such as the Kennedy assassination files, critically impact the product of its systematic review program. Additionally, in FY 1994, FOIA requests for NARA's classified records increased significantly. Since FOIA reviews are far more time intensive than systematic review, the negative impact on NARA's total declassified product was substantial.

The lack of sufficient resources to conduct a viable systematic review program has led to a new approach to deal with the build-up of older, permanently valuable classified records. E.O. 12958 substitutes a structured automatic declassification provision for the page by page, line by line burden of systematic review. As envisioned, systematic reviews will be retained to deal only with those relatively few records exempted from automatic declassification under the new system.

Mandatory Review

Under E. O. 12356, the mandatory review process allows agencies or citizens to require an agency to review specified national security information for purposes of seeking its declassification. Requests must be in writing and describe the information with sufficient detail to permit the agency to retrieve it with a reasonable amount of effort. Mandatory review remains popular with some researchers as a less contentious alternative to Freedom of Information Act (FOIA) requests. It is also used to seek the declassification of the presidential papers or records of former presidents, which are not subject to FOIA.

31% increase

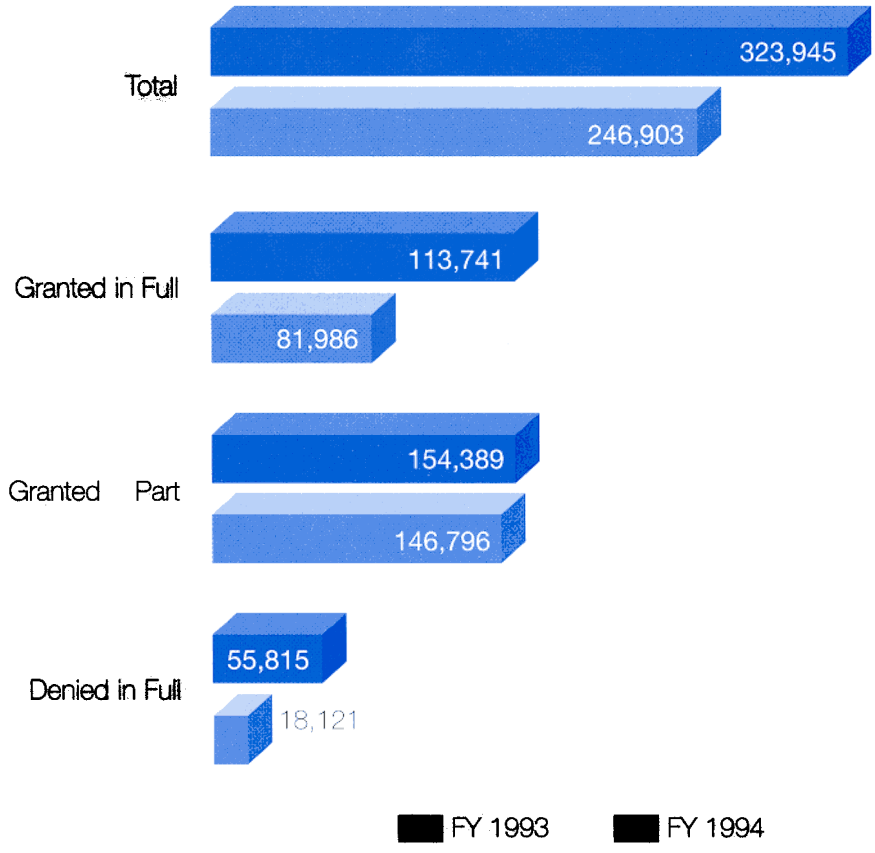
in number of pag

subject to mandat

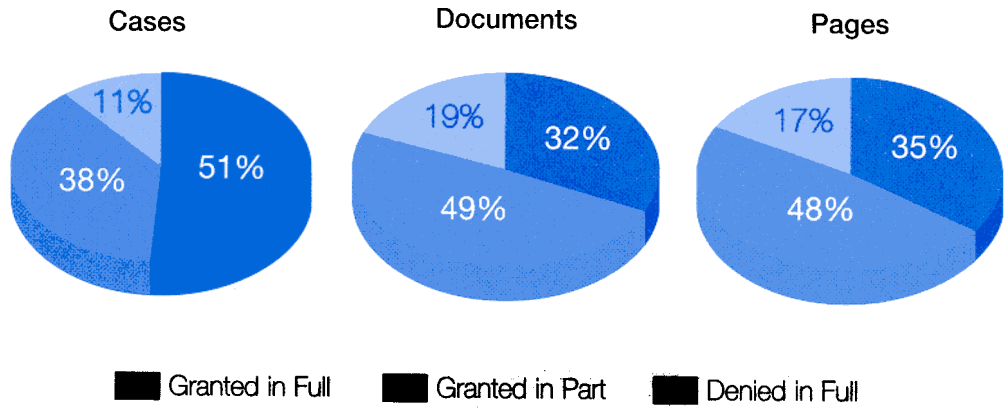
review

The 4,196 cases processed under mandatory review during FY 1994 comprised 51,976 documents totaling 323,945 pages. The number of pages processed represents a 31% increase from the prior year. The percentage of pages declassified in whole or in part (83%) fell significantly from last year's rate of 93%. Given the high proportion and number of pages declassified, mandatory review remains a highly successful mechanism for the declassification of information. With the advent of an Interagency Security Classification Appeals Panel under E.O. 12958, mandatory review may become even more popular in the future.

Mandatory Review Pages Processed FY 1993–1994



Mandatory Review Action Taken FY 1994



E.O. 12356 also provides that agencies or members of the public may appeal mandatory review denials to designated officials of the denying agencies. In FY 1994, the number of documents and pages processed on appeal dropped dramatically. These decreases result from the figures reported by the Department of Justice for mandatory review appeals. During an administrative review of its data collection procedures, the FBI discovered that it had incorrectly included Freedom of Information Act requests in its past reports. Consequently, Justice did not include these requests in its FY 1994 report.

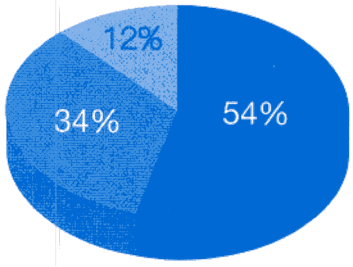
83% of pages declassified in whole or part

During FY 1994, agencies processed 77 appeals that comprised 386 documents totaling 3,046 pages. Of these, 88% of the pages were granted in whole or in part. This high rate suggests that researchers can continue to anticipate greater returns in declassified information if they pursue an appeal.

Mandatory Review Actions By Agency FY 1994

Agency	Total Cases Acted on	%Granted in Full	%Granted in Part	%Denied in Part
DOD	1,154	60	23	17
State	893	52	44	4
CIA	597	38	52	10
NSC	591	53	46	1
NARA	561	40	36	24
DOE	86	3	97	0
All Others	314	73	19	8
Totals	4,196	51	38	11

Mandatory Review Appeals Disposition FY 1994



Total of 3,046 pages processed

Granted in Full Granted in Part Denied in Full

Under E.O. 12958, mandatory review may become an attractive alternative to FOIA

Safeguarding

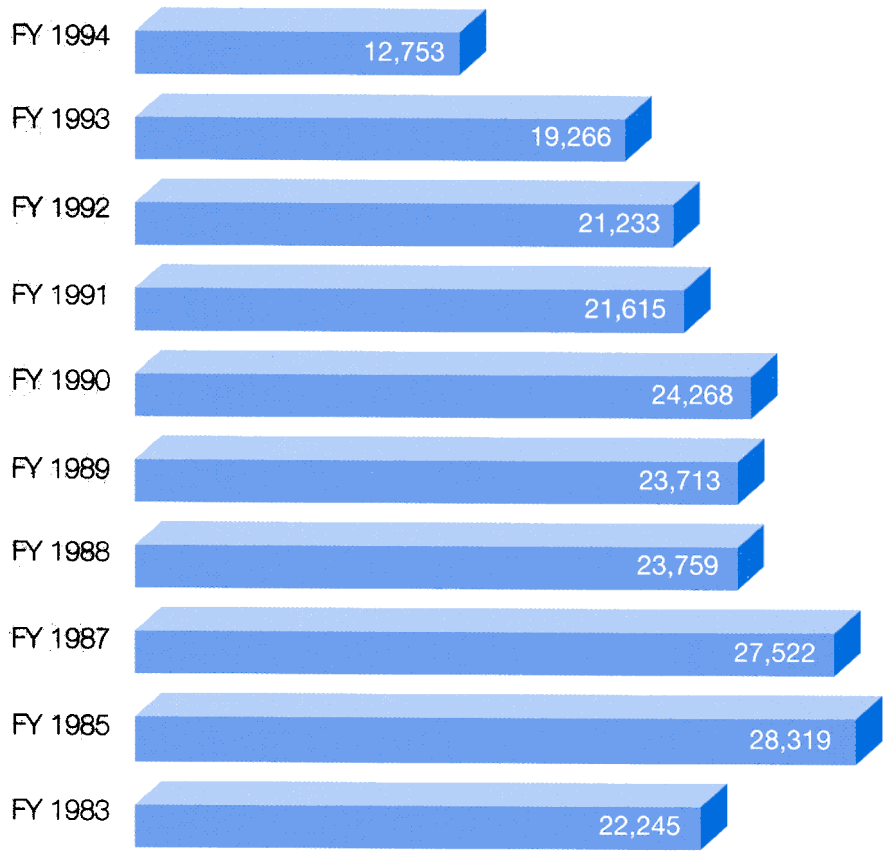
34% fewer agency self-inspections than last year

Executive Order 12356 requires that each executive branch agency that originates or handles classified information establish and maintain "an active oversight and security education program." Self-inspections are an important part of an agency's program and allow it to identify infractions (minor violations) of the Executive Order, the implementing ISOO Directive or agency regulations. Agencies are required to report to ISOO the number and results of these self-inspections each year.

For the fourth year in a row, agencies reported a decrease in the number of self-inspections. For FY 1994, agencies reported 6,513 fewer self-inspections, a 34% decrease from the number reported in FY 1993. This dramatic decrease is largely attributed to DOD, which conducted 5,813 fewer self-inspections in FY 1994 than in FY 1993. Other agencies with significant decreases include CIA, Commerce, DOE, DOT, FEMA, Justice and NASA. These reductions in self-inspections are attributed to downsizing and reorganizations throughout the Government. Those agencies reporting major increases, thus enhancing their oversight capability, include HHS, HUD, NARA, NSF, and State.

In FY 1994, agencies detected a total of 12,961 infractions. Compared to FY 1993, this figure represents a 31% decrease. Although the overall number of inspections has decreased by a substantial margin, the average number of infractions discovered per inspection increased slightly from 0.97 in FY 1993, to 1.02 in FY 1994. While these figures are encouraging, they are not at a level that indicates that an effective self-inspection program is in place at all agencies. Pursuant to sections 5.2 and 5.3 of Executive Order 12958, "Classified National Security Information," an implementing directive for agency self-inspection programs will be issued shortly. ISOO believes that establishing uniform standards for comprehensive self-inspections will improve the quality of agency self-inspection programs as well as the accuracy of statistical data that are annually reported to ISOO.

Agency Self–Inspections



E.O. 12958 will result

uniform self-inspectio

standards

Infractions

Infraction	Total FY 93	Total FY 94
Unauthorized Access	271	509
Mismarking	10,416	5,287
Unauthorized Transmission	1,465	1,333
Improper Storage	5,150	4,490
Unauthorized Reproduction	51	127
Overclassification	683	555
Underclassification	177	91
Classification w/o Authority	33	35
Improper Destruction	141	142
Other	378	392
Totals	18,765	12,961

Executive Order 12958 of April 17, 1995

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

Sec. 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.

Sec. 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 the 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

(2) 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.

Sec. 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.

Sec. 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 con-

sistent 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.

Sec. 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.

Sec. 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 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 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.

Sec. 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 an appropriate manner:

(1) one of the three classification levels defined in section 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 ten 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) Specific 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.

Sec. 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.

(e) 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.

Sec. 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 2 - DERIVATIVE CLASSIFICATION

Sec. 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 establishes 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.

Sec. 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.

Sec. 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 3 - DECLASSIFICATION AND DOWNGRADING

Sec. 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.

Sec. 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.

Sec. 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.

Sec. 3.4. *Automatic Declassification.*

(a) Subject to paragraph (b), below, within five 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 deter-

mined 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.

Sec. 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.

Sec. 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 two years. If the agency has reviewed the information within the past two 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 is 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.

Sec. 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 non-existence of requested information whenever the fact of its existence or non-existence 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.

Sec. 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 4 - SAFEGUARDING

Sec. 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) "Special 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.

Sec. 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.

Sec. 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.

Sec. 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.

Sec. 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 5 - IMPLEMENTATION AND REVIEW

Sec. 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.

Sec. 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.

Sec. 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.

Sec. 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 two 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.

Sec. 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 four 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 from 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.

Sec. 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;

(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 on-going 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.

Sec. 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 6—GENERAL PROVISIONS

Sec. 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.

Sec. 6.2. *Effective Date.* This order shall become effective 180 days from the date of its issuance.

William J. Clinton

Agency Acronyms or Abbreviations

ACDA	: Arms Control and Disarmament Agency
AID	: Agency for International Development
Air Force	: Department of the Air Force
	: Department of the Army
ARPA	: Advanced Research Projects Agency
BIB	: Board for International Broadcasting
CEA	: Council of Economic Advisers
CIA	: Central Intelligence Agency
Commerce	: Department of Commerce
DCAA	: Defense Contract Audit Agency
DIA	: Defense Intelligence Agency
DIS	: Defense Investigative Service
DISA	: Defense Information Systems Agency
DLA	: Defense Logistics Agency
DMA	: Defense Mapping Agency
DNA	: Defense Nuclear Agency
DOD	: Department of Defense
DOE	: Department of Energy
DOT	: Department of Transportation
ED	: Department of Education
EPA	: Environmental Protection Agency
EXIMBANK	: Export-Import Bank of the United States
FBI	: Federal Bureau of Investigation
FCA	: Farm Credit Administration
FCC	: Federal Communications Commission
FEMA	: Federal Emergency Management Agency
FMC	: Federal Maritime Commission
FRS	: Federal Reserve System
	: General Services Administration
HHS	: Department of Health and Human Services
HUD	: Department of Housing and Urban Development
ICC	: Interstate Commerce Commission
Interior	: Department of the Interior
ISOO	: Information Security Oversight Office
ITC	: International Trade Commission
	: Joint Chiefs of Staff

Justice	Department of Justice
Labor	Department of Labor
MMC	Marine Mammal Commission
MSPB	Merit Systems Protection Board
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
Navy	Department of the Navy
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
OA, EOP	Office of Administration, Executive Office of the President
OIG, DOD	Office of the Inspector General, Department of Defense
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
OPIC	Overseas Private Investment Corporation
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
OSIA	On-Site Inspection Agency
OSTP	Office of Science and Technology Policy
OVP	Office of the Vice President
PC	Peace Corps
PFIAB	President's Foreign Intelligence Advisory Board
SBA	Small Business Administration
SEC	Securities and Exchange Commission
SSS	Selective Service System
State	Department of State
Treasury	Department of the Treasury
TVA	Tennessee Valley Authority
USDA	Department of Agriculture
USIA	United States Information Agency
USMC	United States Marine Corps
USPS	United States Postal Service
USTR	Office of the United States Trade Representative
VA	Department of Veterans Affairs

Information Security Oversight Office

750 17th Street, N.W. • Washington, DC 20006 • Phone 202-395-7450 • Fax 202-395-7460