INFORMATION SECURITY OVERSIGHT OFFICE

REPORT TO THE PRESIDENT

2002

June 30, 2003
The President
The White House
Washington, DC 20500

Dear Mr. President:

We are pleased to submit to you the Information Security Oversight Office's (ISOO) 2002 Report.

This Report provides information on the status of the security classification program as required by Executive Order 12958, "Classified National Security Information." It includes statistics and analysis concerning components of the system, primarily classification and declassification. In addition, it contains cost estimates for the security classification system in both Government and industry. Finally, it contains information concerning the implementation of the National Industrial Security Program as required by Executive Order 12829, "National Industrial Security Program."

In response to the current environment of rapidly evolving threats, most agencies have enhanced their systems for safeguarding national security information and protecting the American people and their Government. At the same time, to ensure the continued integrity of the classification system, agencies must be more discerning in how much and how long information is classified. Your recent amendment to Executive Order 12958 gives direction and renewed emphasis to how long information is classified by requiring agencies to make the concept of automatic declassification of historical records that are more than 25 year old a reality by December 31, 2006. Most agencies will need to step up their declassification activities in the coming years to fulfill this directive. Finally, continual refinements in the classification system are required to move the executive branch to a nearly seamless framework that addresses the twin imperatives of information sharing and information protection in the information age.

The National Industrial Security Program (NISP) is in need of a renewed commitment to its goals of administering an integrated and cohesive program that safeguards classified information while preserving our Nation's economic and technological interests. Both Government and industry must redouble their efforts to administer and manage the NISP so that it is responsive and supportive of the Government's transformation activities. Without this commitment, the goals of the NISP will not be fully realized.

Many thousands of individuals within Government and industry are responsible for the progress made thus far in implementing E.O. 12958 and E.O. 12829. There is more that needs to be done and these same individuals stand ready to support your programs to promote an informed American public and to protect our national security.

Respectfully,

J. William Leonard
Director

Information Security

AUTHORITY

Executive Order 12958, "Classified National Security Information," and Executive Order 12829, "National Industrial Security Program." The Information Security Oversight Office (ISOO) is a component of the National Archives and Records Administration and receives its policy and program guidance from the National Security Council (NSC).

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, along with other information, reports them annually 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.
- Recommends policy changes to the President through the NSC.
- Provides program and administrative support for the Interagency Security Classification Appeals Panel (ISCAP).

OVERSIGHT OFFICE

GOALS

- Promote and enhance the system that protects the national security information that safeguards the American government and its people.
- Provide for an informed American public by ensuring that the minimum information necessary to the interest of national security is classified and that information is declassified as soon as it no longer requires protection.
- Promote and enhance concepts that facilitate the sharing of information in the fulfillment of mission critical functions related to national security.

Summary of FY 2002 Program Activity*

The following Report to the President is the seventh report under E.O. 12958, which went into effect in October 1995. The following data highlight ISOO's findings.

CLASSIFICATION

- Executive branch agencies reported 4,006 original classification authorities.
- Agencies reported 217,288 original classification decisions.
- Executive branch agencies reported 23,528,041 derivative classification decisions.
- Agencies reported 23,745,329 combined classification decisions.

DECLASSIFICATION

- Under Automatic and Systematic Review Declassification programs, agencies declassified 44,365,711 pages of historically valuable records.
- Agencies received 3,424 new mandatory review requests.
- Under mandatory review, agencies declassified in full 52,945 pages; declassified in part 97,270 pages; and retained classification in full on 14,435 pages.
- Agencies received 81 new mandatory review appeals.
- On appeal, agencies declassified in whole or in part 4,422 additional pages.

*Please see page 17 for an explanation concerning DOD's security classification program data for FY 2001 and a clarification of ISOO's FY 2001 Annual Report data.

Table of Contents

A Look to the Future of the Security Classification System in a Post 9/11 Environment

Our Nation and our Government are profoundly different in a post 9/11 world. Americans' sense of vulnerability has increased, as have their expectations of their Government to keep them safe. Information is crucial to responding to these increased concerns and expectations. On the one hand, Americans are concerned that information may be exploited by our country's adversaries to harm us. On the other hand, impediments to information sharing among Federal agencies and with state, local and private entities need to be overcome in the interests of homeland security. Equally so, the free flow of information is essential if citizens are to be informed and if they are to be successful in holding the Government and its leaders accountable. In many ways, the Federal government is confronted with the twin imperatives of information sharing and information protection, two notions that contain inherent tension but are not necessarily contradictory.

Each year this report seeks to highlight possible trends with respect to the amount of information produced by the executive branch that is beyond the American public's immediate purview because it is classified. In FY 2002 much of the executive branch's attention and action focused on the global war on terrorism and on homeland security related issues. These issues have contributed to a reported increase of 14 percent in the number of classification decisions made by classifiers in the executive branch as compared to FY 2001.

An increase in classification activity can be expected in times of crisis, when the potential for the loss of life if national security information is improperly disclosed is more than theoretical. Effective classification can protect the intelligence source or method required to detect and preclude the next terrorist event. It also can save the lives of our Service men and women who place themselves in harm's way to defend our Nation. Furthermore, Government agencies have found it necessary to examine their mission responsibilities in new ways in order to understand their vulnerability to terrorist and other hostile attacks. This has resulted in new authorities and more classification decisions.

Nonetheless, when it comes to classification activity, more is not necessarily better. Much the same way the indiscriminate use of antibiotics reduces their effectiveness in combating infections, classifying either too much information or for too long can reduce the effectiveness of the classification system, which, more than anything else, is dependent upon the confidence of the people touched by it. While there is always a temptation to err on the side of caution, especially in times of war, the challenge for agencies is to similarly avoid damaging the nation's security by hoarding information.

Both consumers and producers of classified information, as well as the general public, need to be assured that the classification system is discerning enough to capture only that information that needs protection in the interest of our national security. If the system is not perceived as being discerning, then the very people depended upon to make the system work begin to substitute their own judgment in determining what is sensitive and requires protection and what is not. This can lead to a lack of accountability, and an environment conducive to unauthorized disclosures of classified information, thus placing all classified information at increased risk of unauthorized disclosure.

While great emphasis is often placed on the consequences of the improper disclosure of classified information, restrictions on dissemination of information carry their own risks. Whether within the Federal Government or between the Federal Government and state, local and private sector personnel, or with the public, the ability to share information rapidly and seamlessly can make the difference in precluding or responding to the next terrorist event. Classification can be a significant impediment to information sharing. As such, there will be situations when just because information *can* be classified, it does not mean that it *should* be classified. Many agencies have recognized the importance of having aggressive downgrading, declassification, and/or sanitization (i.e., removal of classified references) programs that promote information sharing at all levels.

Today's rapidly changing environment suggests that the current framework for identifying, protecting and declassifying national security information is due for some fundamental reassessment. In addressing the imperatives of information sharing and information protection, special note must be made of the electronic environment in which the Government increasingly operates. As Government agencies reengineer their business processes and then apply information technology solutions, they are often still unable to effectively communicate and share information with another agency. This can be due, in part, to the fact that they superimpose upon their new processes a document-centric process for classifying information that has fundamentally remained unchanged for the past 60 years.

Our current challenge, then, is to be able to recast existing policy governing the classification of information to reflect the Government's electronic operating environment. This will require the transformation of the current document-centric framework for classifying information requiring protection in the interest of national security to one more conducive to information sharing taking into account the life-cycle of information. The Information Security Oversight Office is preparing now to embark on this challenge, seeking innovative solutions through the interagency process for this important policy of the future.

Interagency Security Classification Appeals Panel

AUTHORITY

Section 5.4 of Executive Order 12958, "Classified National Security Information."

FUNCTIONS

(1) To decide on appeals by authorized persons who have filed classification challenges under Section 1.9 of E.O. 12958.

(2) To approve, deny or amend agency exemptions from automatic declassification as provided in Section 3.4(d) of E.O. 12958.

(3) To decide on mandatory declassification review appeals by parties whose requests for declassification under Section 3.6 of E.O. 12958 have been denied at the agency level.

MEMBERS*

William H. Leary,
Acting Chair
National Security Council

James A. Baker
Department of Justice

Carl A. Darby
Intelligence Community

Carol A. Haave
Department of Defense

Michael J. Kurtz
National Archives and Records Administration

Frank M. Machak
Department of State

EXECUTIVE SECRETARY*

J. William Leonard,
Director, Information Security Oversight Office

SUPPORT STAFF

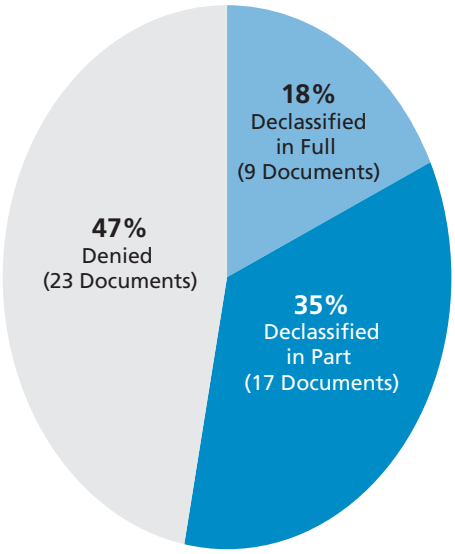
Information Security Oversight Office

SUMMARY OF ACTIVITY

The Interagency Security Classification Appeals Panel (ISCAP) was created under E.O. 12958 to perform the critical functions noted in this section. The ISCAP, comprised of senior level representatives appointed by 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, began meeting in May

**The individuals named in this section were those in such positions as of the end of FY 2002.*

ISCAP Decisions
Fiscal Year 2002



1996. The President designates its Chair; the Director of ISOO serves as its Executive Secretary, and ISOO provides its staff support.

To date, the majority of the ISCAP's efforts have focused on mandatory declassification review appeals. During FY 2002, the ISCAP decided upon 49 documents that remained fully or partially classified upon the completion of agency processing. It declassified the entirety of the remaining classified information in 9 documents (18%), and declassified some portions, while affirming the classification of other portions, in 17 of the documents (35%). The ISCAP fully affirmed the agency decisions in their entirety for 23 documents (47%).

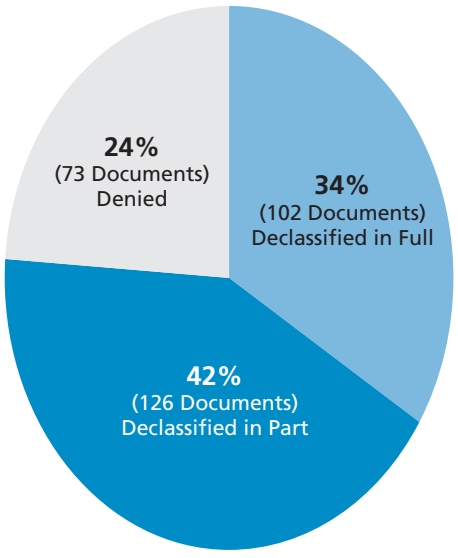
From May of 1996 through September 2002, the ISCAP has decided upon a total of 301 documents. Of these, the ISCAP declassified information in 76% of the documents. Specifically, it has declassified the entirety of the remaining classified information in 102 documents (34%), and has declassified some portions, while affirming the classification of other portions, in 126 documents (42%). The ISCAP has fully affirmed agency classification actions in 73 documents (24%).

Documents declassified by the ISCAP are made available through the entity that has custody of them, usually a presidential library. For assistance in identifying and requesting copies of such documents, or for any other questions regarding the ISCAP, please contact the ISCAP staff at ISOO.

The ISCAP also approved a declassification guide submitted by the Department of the Treasury in accordance with Section 3.4(d) of E.O. 12958 and the applicable provision of its government-wide implementing directive (32 C.F.R. Part 2001.51(i)). When approved by the ISCAP, such guides authorize the exemption of information determined by an agency to fall within an exemption category listed in Section 3.4(b) of the Order. Essentially, the guides permit certain information to be classified for more than 25 years. In order for the ISCAP to approve a guide it must provide: a comprehensive description of the information proposed for exemption; a distinct relationship to a specific exemption; a rational justification or explanation of the need for exemption; and a fixed date or event for future declassification.

During this period, the ISCAP heard its first appeal of a classification challenge

ISCAP Decisions
May 1996 - September 2002



filed pursuant to Section 1.9 of E.O. 12958. This appeal sought to reverse the decision of the Defense Department that four portions of an abstract regarding Global Positioning System Monitor Station data were classified. As the information was less than 10 years old and concerned "vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security," the ISCAP affirmed the prior classification of each of the portions under Section 1.5(g) of the Order.

If you have any questions concerning the ISCAP, please contact the ISCAP staff at:

Telephone .....(202) 219 - 5250
Fax .....(202) 219 - 5385
E-mail .....iscap@nara.gov
Internet .....http://www.archives.gov/isoo/oversight_groups/iscap.html

The National Industrial Security Program

Executive Order 12829 of January 6, 1993, established the National Industrial Security Program (NISP). Its goal, then and now, is to make the executive branch's industrial security program more efficient and cost effective while fully protecting classified information in the possession of Government contractors, licensees or grantees. The NISP is intended to serve as a single, integrated, cohesive industrial security program and to ensure that short and long-term costs of requirements, restrictions and other safeguards are taken into account in the program's implementation.

In the ten years that the NISP has been in existence, it has yet to achieve its full potential. Three areas of concern continue to prevent the NISP from reaching its full potential:

- **Clearance delays.** Investigative and adjudicative delays totaling a year or more are still common. The clearance processing delays experienced by industry have serious consequences for both industry and its Government customers. While both Government and industry have had to deal with these long standing challenges, industry is more limited in its ability to respond.

- **Reciprocity.** While reciprocity is a major tenet of the NISP, from industry's perspective, it is not being practiced consistently. Reciprocity means the acceptance of clearance certifications between and among agencies without levying additional requirements. The lack of reciprocity creates duplicative efforts, lengthy time delays, and inefficient use of valuable resources.

- **Automated Information Systems (AIS) Accreditation.** Accreditation of AIS has been a problem area for both Government and industry alike. Industry continues to report difficulty in this area, in particular, the considerable delays in the system accreditation process. These delays stem from the availability of resources to perform the accreditations. Other concerns in this area relate to the consistency in the interpretation and application of the AIS requirements set forth in Chapter 8 of the NISP Operating Manual.

The impact of these issues are obvious: considerable additional costs to both contractors and their Government customers, as well as limiting industry's ability to recruit and retain the best and the brightest. Collectively, these issues limit industry's ability to respond to Government's needs in a timely manner. Ultimately, they

negatively effect Government's and industry's ability to optimize both budget and technology to maintain this country's position as a leader on the global stage.

Several initiatives are being developed or implemented to address these longstanding issues, to include consolidating the function for most security investigations into one entity. The signatories of the NISP, the Departments of Defense and Energy, the Central Intelligence Agency and the Nuclear Regulatory Commission will be critical players in the success or failure of these initiatives.

The National Industrial Security Program Policy Advisory Committee (NISPPAC), also established by Executive Order 12829,[1] serves an important role by bringing forward issues and possible solutions concerning the NISP. By bringing together Government and industry, the NISPPAC can facilitate equitable resolutions to common problems.

In keeping with the oversight responsibilities for the NISP, ISOO will develop a Government-wide implementing directive for the NISP through an interagency effort. ISOO anticipates playing a greater role in facilitating information sharing between Government and industry through increased liaison activity.

For more information on NISP initiatives go to ISOO's home page at http://www.archives.gov/isoo/oversight_groups/nisp.html

[1] *The NISPPAC is chaired by the Director of ISOO. It is made up of 24 members, including 8 members from industry and 16 Government members. The NISPPAC advises the Director of ISOO on all matters concerning the policies of the NISP, including recommending changes to those policies. The NISPPAC also serves as a forum for discussing policy issues in dispute.*

Security Classification: What Does It Cost?

The security classification program is now in its eighth year of reporting costs for both Government and industry. Congress first requested security classification cost estimates from the executive branch in 1994. In addition, ISOO is tasked through Executive Order 12958 to report these costs to the President. Executive Order 12829, also requires that industry or contractor costs be collected and reported by ISOO to the President.

Until the last few years, the costs for the security classification program were deemed non-quantifiable, intertwined with other somewhat amorphous overhead expenses. While many of the program's costs remain ambiguous, ISOO continues to monitor the methodology used to collect the cost estimate data. Requiring agencies to provide exact responses to the cost collection efforts would be cost prohibitive. Consequently, ISOO relies on sampling to estimate the costs of the security classification system. The collection methodology has remained stable over the past eight years providing a good indication of the trends in total cost. In the future, ISOO expects to review the cost collection methodology, particularly the definitions being used. This review will help to ensure that the methodology is current and relevant.

GOVERNMENT

The data presented below were collected by categories based on common definitions developed by an executive branch-working group. The categories are defined below.

Personnel Security: A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

Physical Security: That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

INFORMATION SECURITY:

INCLUDES THREE SUB-CATEGORIES:

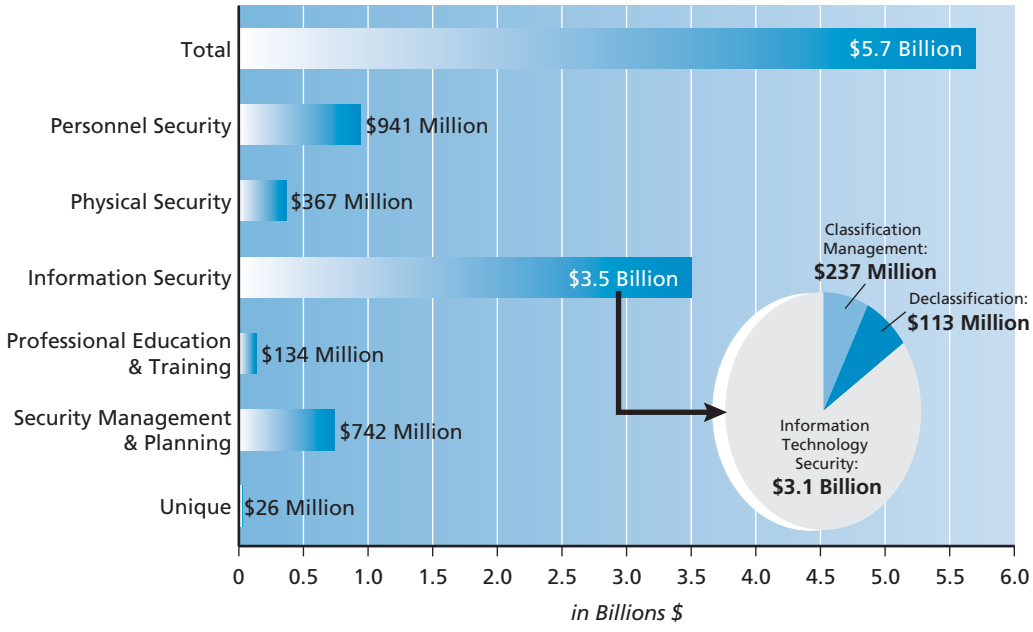
Classification Management: The system of administrative policies and procedures for identifying, controlling and protecting classified information from unauthorized disclosure, the protection of which is authorized by executive order or statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, or destroy classified information.

Declassification: The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic or mandatory review programs authorized by executive order or statute.

Information Technology Systems Security (Automated Information Systems or Information Technology Systems Security): Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer or information technology system. It can include, but is not limited to, the provision of all security features needed to provide an accredited system of protection for computer hardware and software, and classified information, material, or processes in automated systems.

Professional Education, Training and Awareness: The establishment, maintenance, direction, support and assessment of a security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated

Government Security Classification Costs Estimate



with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

Security Management and Planning: Development and implementation of plans, procedures and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities and respond to management requests related to classified information.

Unique Items: Those department or agency specific activities that are not reported in any of the primary categories but are nonetheless significant and need to be included.

The total security classification costs estimate within Government for FY 2002 is $5,688,385,711. This figure represents estimates provided by 45 executive branch agencies, including the Department of Defense, whose estimate incorporates the National Foreign Intelligence Program. It does not include, however, the cost estimates of the CIA, which that agency has classified.

Because of expressed interest in the declassification programs established under Executive Order 12958, ISOO also requested agencies to identify that portion of their cost estimates in the category of information security/classification management that was attributable to their declassification programs. For FY 2002, the agencies reported declassification cost estimates of $112,964,750, or 2 percent of their total cost estimates, which is a significant drop from last year's 4.9 percent.

INDUSTRY

A joint Department of Defense and industry group developed a cost collection methodology for those costs associated with the use and protection of classified information within industry. Because industry accounts for its costs differently than Government, cost estimate data are not provided by category. Rather, a sampling method was applied that included volunteer companies from four different categories of facilities. The category of facility is based on the complexity of security requirements that a particular company must meet in order to hold a classified contract with a Government agency.

The 2002 cost estimate totals for industry pertain to the twelve-month accounting period for the most recently completed fiscal year of each company that was part of the industry sample. For most of the companies included in the sample, December 31, 2002, was the end of their fiscal year. The estimate of total security costs for 2002 within industry was $839,809,000.

The Government cost estimate shows a 21 percent increase above the cost estimate reported for FY 2001. Industry also reported a 10 percent increase in its cost estimate from calendar year 2001. The total cost estimate for Government and industry for 2002 is $6.5 billion, $1 billion more than the total cost estimate for Government and industry in 2001.

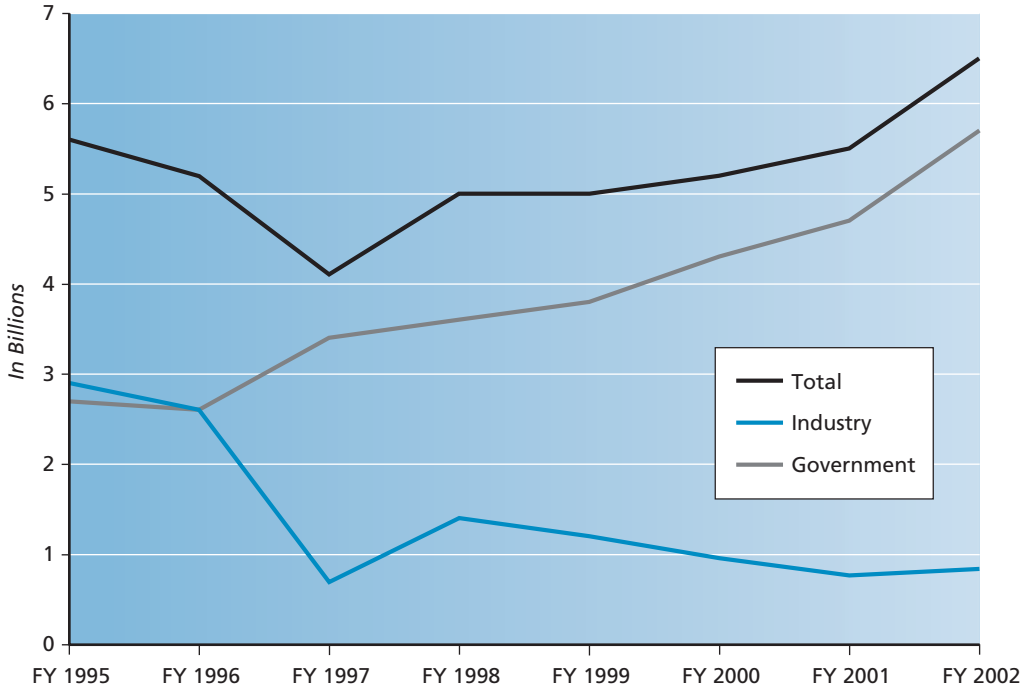
The increase in cost estimates for Government can be attributed, in part, to greater attention to security programs after September 11, 2001; in particular, Physical Security cost estimates went up by 70 percent. All other categories noted increases, Personnel Security (9%); Professional Education, Training and Awareness (21%);

Security Management, Oversight and Planning (31%); Unique Items (2%); Information Security/Classification Management (7%); and Information Technology (20%), except Declassification, which saw a 50 percent decrease from last year. Given the events of September 11th, this could be expected. However, the decrease in declassification activity is an area of concern that the Information Security Oversight Office will monitor closely. While it seems reasonable that some funding for the declassification program would be deferred in the short term, it cannot continue to decline, or significant amounts of classified information will remain unreviewed when it becomes subject to automatic declassification on December 31, 2006.

For the first time in 3 years, contractor costs have risen. The 2002 figure is not the highest reported by industry, but represents the high middle ground for industry. This increase in cost estimates for industry is more than likely also a reflection of post 9/11 requirements. The current estimate was again based on sampling from a larger pool of companies. ISOO continues to believe, as does the Executive Agent for the National Industrial Security Program (Department of Defense), that a larger mix of small and large companies reporting data would provide a better sample. ISOO expects that future estimates will continue to include this larger mix of small and large companies, which appears to yield the most realistic and consistent data reported to date.

Comparing Total Costs for Government and Industry

Fiscal Years 1995-2002



Classification

CLARIFICATION OF FISCAL YEAR 2001 DATA

In ISOO's FY 2001 *Annual Report* some of the data reported for the Department of Defense's security classification program were incorrect. We fully recognize the significance of this error and have taken steps to ensure that it does not recur. ISOO and all agencies will continue to work together closely to make certain that all data are valid, are reported accurately, and are of value to those interested in such data.

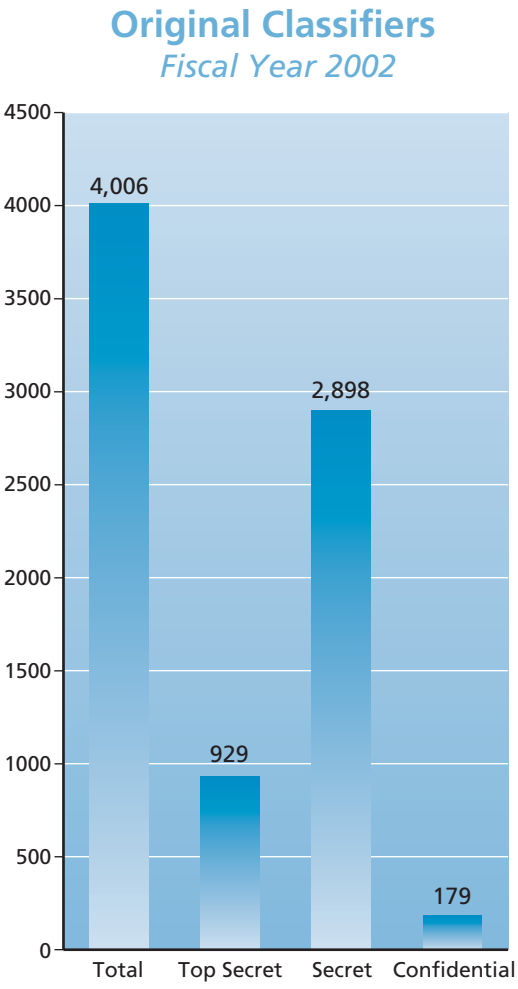
Certain areas of last year's annual report are little affected by the correction in DOD figures, such as the number of original classification authorities, number of original classification decisions, and pages declassified under mandatory review appeals. The sections regarding derivative classification actions and mandatory review requests are significantly impacted, however. In those cases where the figures make a significant difference in how the data should be interpreted, ISOO includes a discussion of the changes within the body of this report. Additionally, we have included charts showing the new figures on pages 24 and 30. ISOO, as noted above, worked closely with OSD to validate the DOD program figures for FY 2002.

ORIGINAL CLASSIFIERS

Original classification authorities (OCAs), 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 Executive Order 12958, only original classifiers determine what information, if disclosed without authority, could reasonably be expected to cause damage to the national security. Original classifiers must also be able to identify or describe the damage.

For fiscal year 2002, the number of original classifiers throughout the executive branch decreased to 4006, or approximately 3 percent from the previous year. Executive branch agencies with significant decreases in OCAs include the Department of Energy (DOE), the Department of Defense (DOD) and the Nuclear Regulatory Commission (NRC). Additionally, the Department of State (State) experienced a slight decrease in the number of OCAs. ISOO believes that the agency heads' careful scrutiny and re-issuance of delegations of original classification authority continues to be the largest contributing factor for keeping OCAs to a minimum. Additionally, the use of classification guidance has reduced the need for OCAs for operational needs.

Nevertheless, some larger agencies that had comparable classification activity, but many more OCAs, could apparently reduce the number of OCAs without negatively affecting operations through the development and increased use of classification guidance. ISOO is pleased to report that the three agencies which received original classification authority for the first time in this fiscal year, the Environmental Protection Agency (EPA), the Department of Health and Human Services (HHS), and the Department of Agriculture (USDA), have exercised great restraint in use of the original classification authority. EPA and USDA have appointed one OCA each, and HHS has appointed three.



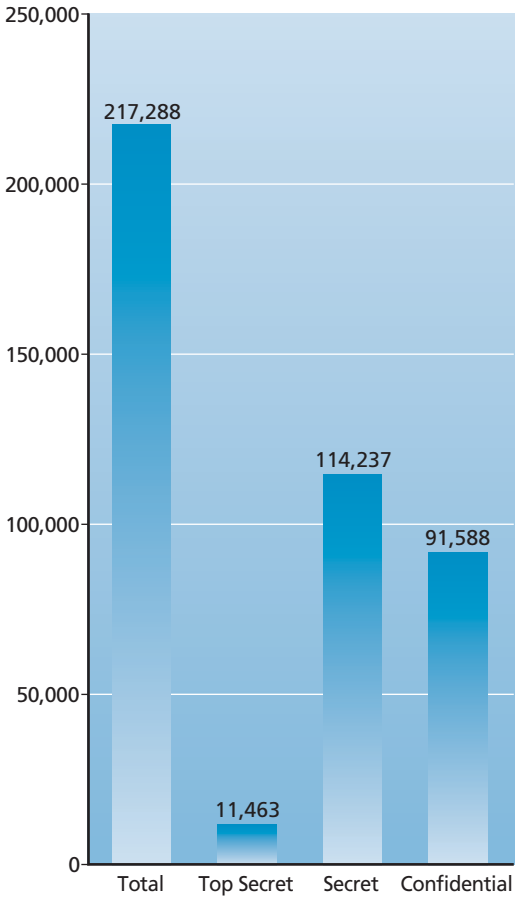
In fiscal year 2002, agencies reported a 5 percent decrease in the number of original classifiers for the Top Secret level, the first decrease in three years. There was a decrease for the Secret level of original classifiers of 2 percent, and a decline of 5 percent at the Confidential level. The number of OCAs in DOD at each of the three levels dropped significantly. This might be in part due to a recent self-review of selected Department of Defense OCA allocations. While most agencies are reducing the number of OCAs, ISOO is concerned that the National Security Council (NSC) increased its overall total by 14 percent and that the National Aeronautics and Space Administration (NASA) increased its overall total by 50 percent. NSC's increase is due in part to the demands of dealing with the issues of global terrorism and homeland security. Because NASA has a small number of OCAs, any increase appears significant. ISOO notes that the Department of Treasury reported a 3 percent increase in its total number of OCAs, and State reported a 2 percent decrease. Although ISOO anticipated a significant increase in the number of OCAs reported by the agencies in FY 2002 as the full effect of our new security environment in a post 9/11 world becomes apparent in the security classification, these figures do not reflect such an increase. ISOO commends the entire Executive Branch for its judicious use of Original Classification Authority.

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

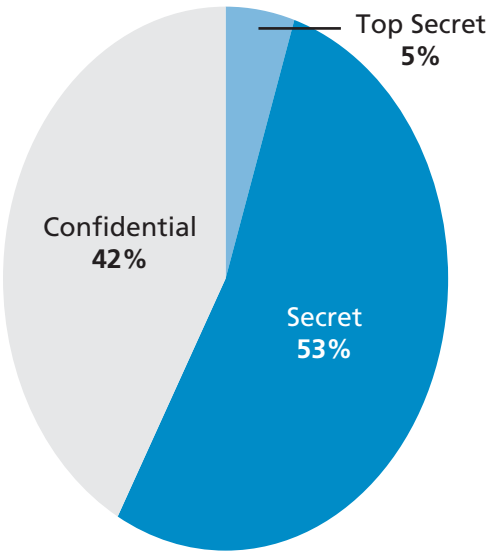
need to protect the information and the placement of markings to identify the information as classified. By definition, original classification precedes all other aspects of the security classification system, e.g., derivative classification, safeguarding, and declassification. Therefore, ISOO often refers to the number of original classification decisions as the most important figure that it reports.

Original Classification Activity
Fiscal Year 2002



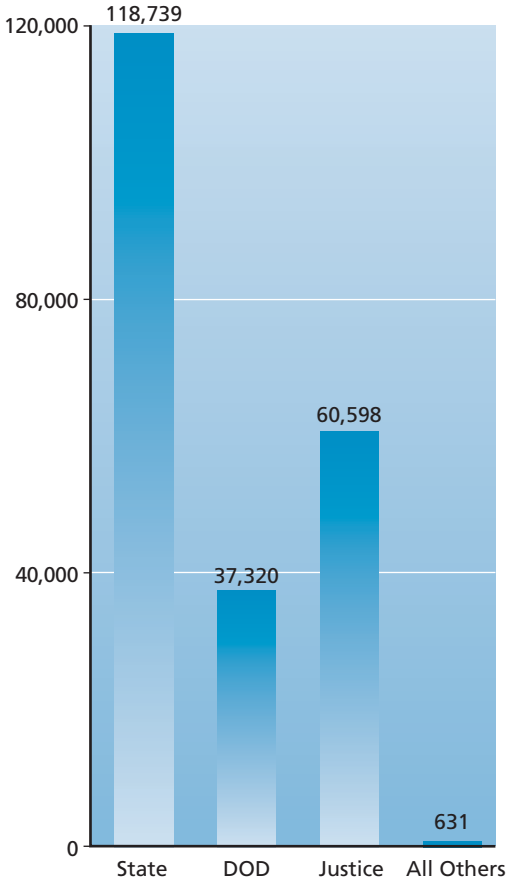
For fiscal year 2002, agencies reported a total of 217,288 original classification decisions. This figure represents a decrease of 17 percent over the number of original classification decisions reported in FY 2001, most of which is attributable to decreases reported by the DOD. By classification level, Top Secret decreased by 4 percent, Secret decreased by 26 percent and Confidential decreased by 2 percent. A review of original classification activity under E.O. 12958 does not show a consistent trend. During fiscal year 1997, the second full year of implementation of the Order, original classification activity increased by 51 percent, while fiscal year 1998 saw a decrease of 14 percent, and fiscal year 1999 an increase of 24 percent. Original classification activity increased by 30 percent in FY 2000 and by 18 percent in FY 2001. The decrease for fiscal year 2002 may continue to reflect changes in how certain agencies are collecting the data but can also reflect transformation in the way agencies accomplish their mission.

Original Classification by Level
Fiscal Year 2002



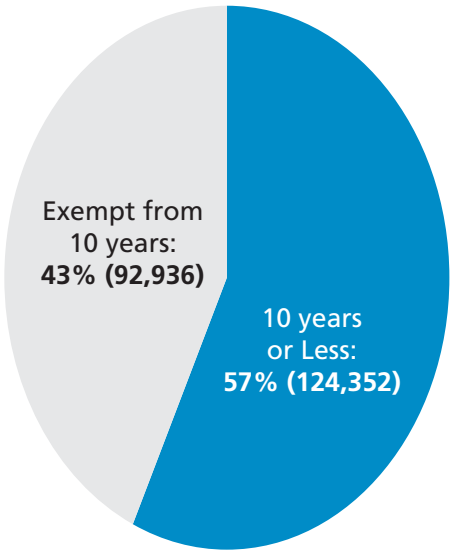
Three agencies—DOD, Justice, and State—now account for 99 percent of all original classification decisions. DOD reported a total of 37,320 original classification decisions, a 59 percent decrease from the previous year. The reasons for the decrease include better education among DOD components on how to report the actions, better accountability of the actual numbers submitted, and increased use of classification guides. For the sixth year in a row, Justice reported an increase. For fiscal year 2002 the increase is directly related to the FBI's activities with the war on terrorism and the Bureau's increased presence in this

Original Classification by Agency



Duration of Classification

Fiscal Year 2002



executive branch-wide effort. State registered a 10 percent increase, probably because of its enhanced accountability and reporting system for this type of information.

Several agencies with smaller security classification programs reported marked decreases in the number of original classification decisions. In particular, ISOO commends AID for a 77 percent decrease. ISOO also notes decreases for Commerce (13%), NASA (37%), ONDCP (27%), OSTP (100%), and Treasury (18%).

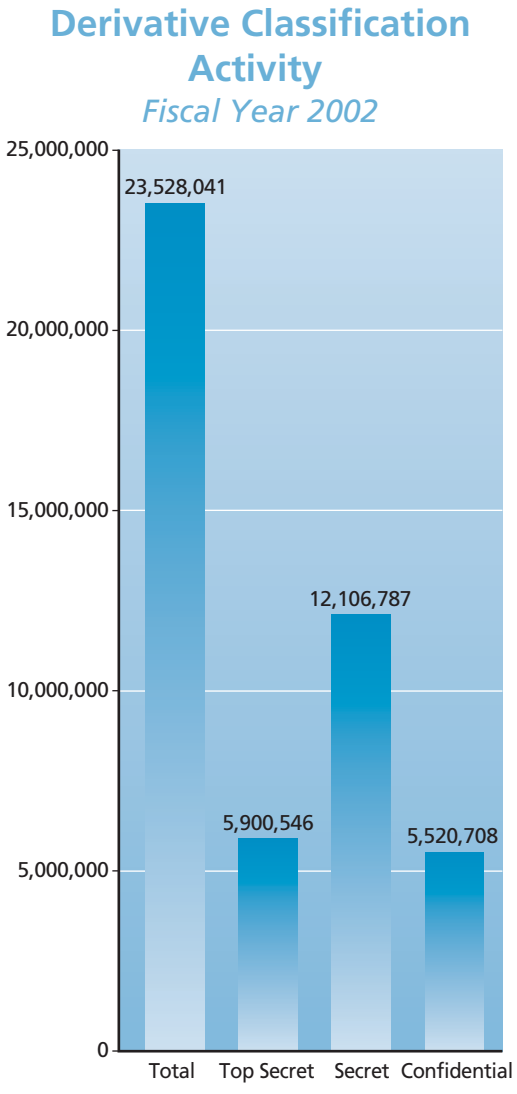
As part of the original classification process, the classifiers must determine a timeframe for the protection of the information. This is commonly called the "duration" of classification. Executive Order 12958 creates three possible outcomes at the time of original classification. First, if applicable to the duration of the information's national security sensitivity, information should be marked for declassification upon a specific date or event. For example, a classifier could determine that the information's sensitivity would lapse upon the completion of a particular project. The event would be noted on the face of the document, and when the project had been completed, the information would automatically be declassified. Second, if the original classification authority could not determine an earlier specific date or event for declassification, information should ordinarily be marked for declassification 10 years from the date of the original decision. Third, if the specific information falls within one or more of eight categories, the classifier may exempt it from declassification at 10 years. In almost all instances, this will result in the information being subject to automatic declassification at 25 years. The indefinite duration marking used under E.O. 12958's predecessor, Executive Order 12356,

"Originating Agency's Determination Required" or "OADR," was eliminated with the issuance of E.O. 12958.

During fiscal year 2002, classifiers chose declassification upon a specific date or event less than 10 years, or upon the 10-year date for 124,352 (57%) original classification decisions. On the remaining 92,936 (43%) original classification decisions, original classifiers elected to apply an exemption from 10-year declassification. The 57 percent noted for the 10-year or less category is only 2 percent lower than the alltime high percentage reported by the agencies in 2000. Historically, under this Order, agencies selected 10 years or less 59 percent in 2000; 50 percent in 1999; 36 percent in 1998 and 50 percent in 1997 and 1996. The 10 years or less timetable seems well accepted by OCAs and should continue. The long-term effect of assigning a specific date, event or 10-year date suggests that more information will be declassified earlier without the need for more costly reviews in the future.

DERIVATIVE CLASSIFICATION

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

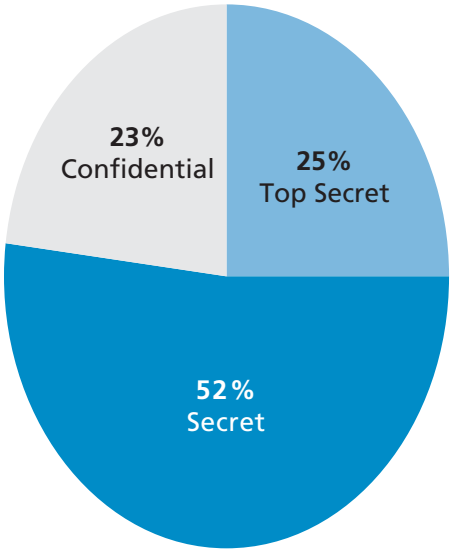


For fiscal year 2002, agencies reported 23,528,041 derivative classification actions. Last year's figure, inaccurately reported in the FY 2001 annual report as 32,760,209, was 20,575,135. The following analysis compares this year's figure with the corrected figure from FY 2001.

This year derivative classification is up 14 percent from last year. The majority of the increase comes from three of the major classifying agencies, DOD, CIA, and

Derivative Classification by Levels

Fiscal Year 2002

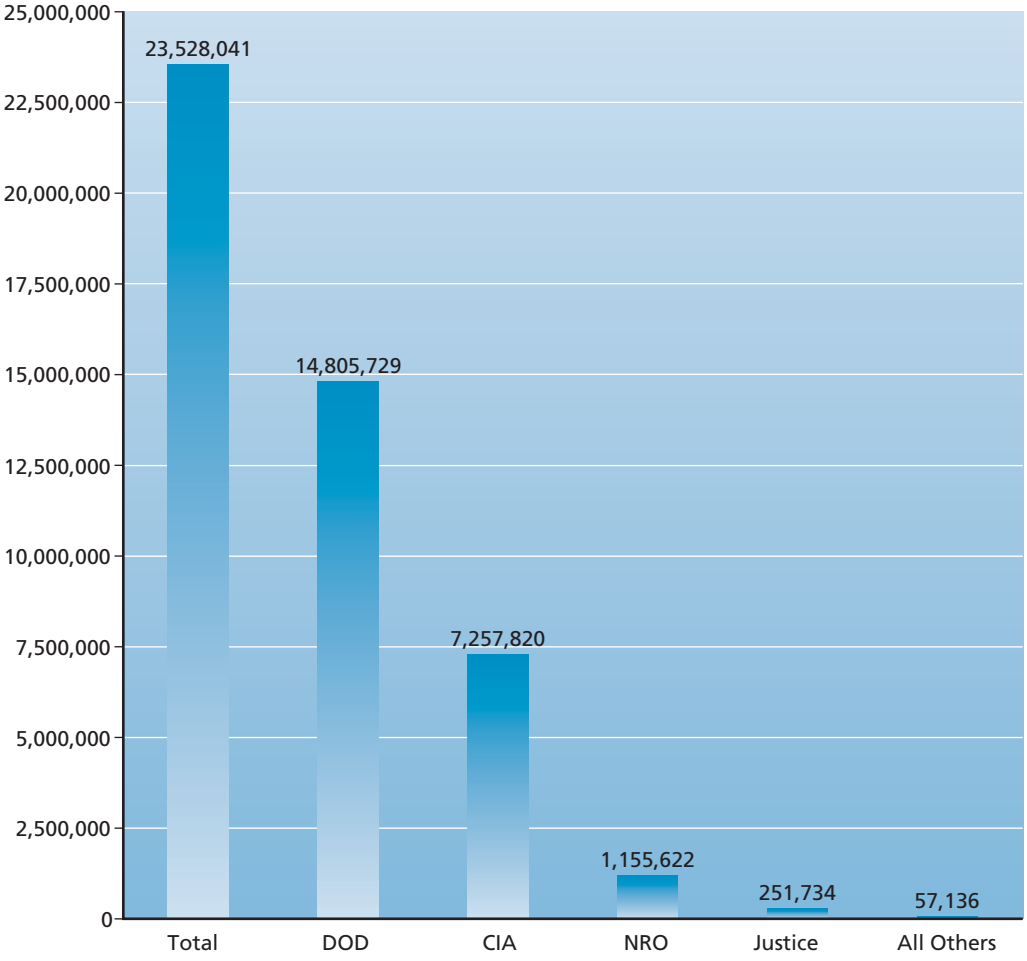


Justice. DOD is up 10 percent, CIA 29 percent, and Justice 52 percent. For fiscal year 2002, DOD, CIA, NRO and Justice represented 99 percent of all derivative classification actions reported. DOD derivatively classified the most of any agency, CIA the second most, NRO the third, with Justice a distant fourth. In addition to NRO, State, Interior and Commerce reported significant decreases. Treasury reported a modest decrease. ISOO commends these agencies for their efforts to reduce derivative classification activity.

The increase in derivative classification activity is influenced by a variety of factors. World events continue to influence the amount of derivative activity, in particular, the global war on terrorism, and homeland security. However, ISOO

Derivative Classification Activity by Agency

Fiscal Year 2002



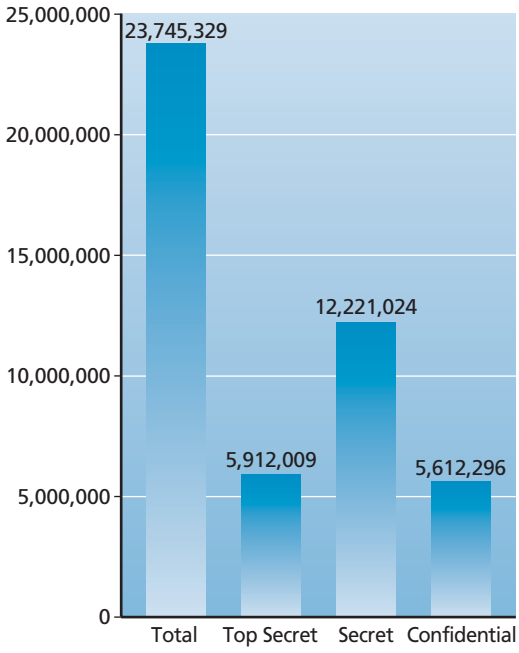
remains convinced that the vastly increased use of automated information management systems, and advancements in technology will continue to affect how information is created, collected, analyzed, and disseminated, thus affecting the tabulation of derivative classification activity. ISOO is continuing to develop guidance for standardization of sampling and the application of what constitutes a classification decision.

COMBINED CLASSIFICATION

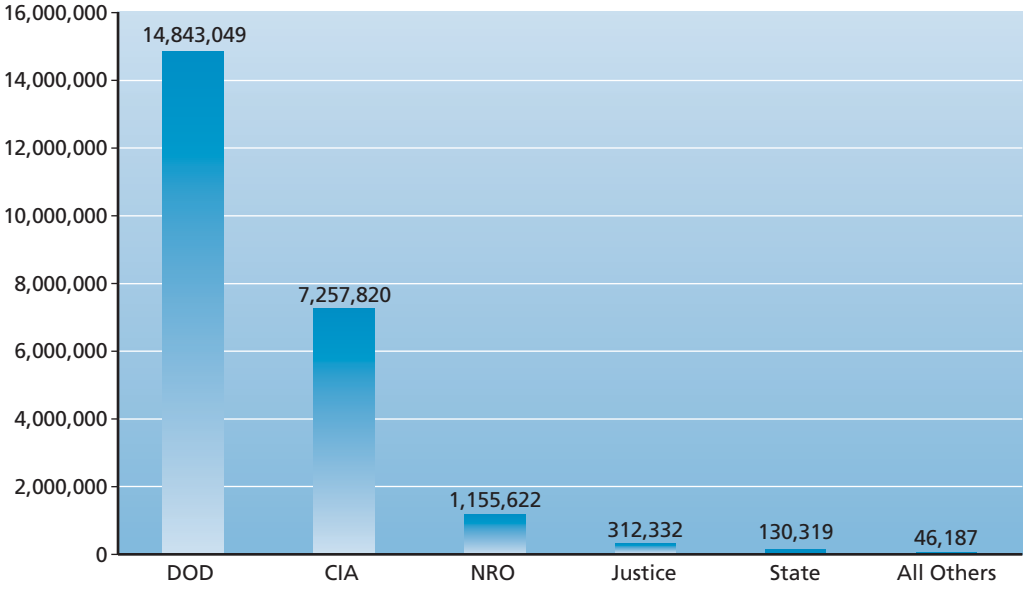
Together, original and derivative classification decisions make up what ISOO calls combined classification activity. In fiscal year 2002, combined classification activity totaled 23,745,329. Since derivative actions outnumbered original actions by a ratio of more than 109:1, the fluctuation in derivative activity essentially determines the fluctuation of combined classification activity.

DOD accounted for 63 percent of all combined classification activity reported for fiscal year 2002; CIA, 30 percent; NRO, 5 percent; and Justice, 1 percent. As in the past, the remaining agencies accounted for only one percent of the combined classification activity. DOD and CIA reported increases in combined classification by 10 and 29 percent, respectively. NRO reported a decline of

Combined Classification Activity
Fiscal Year 2002

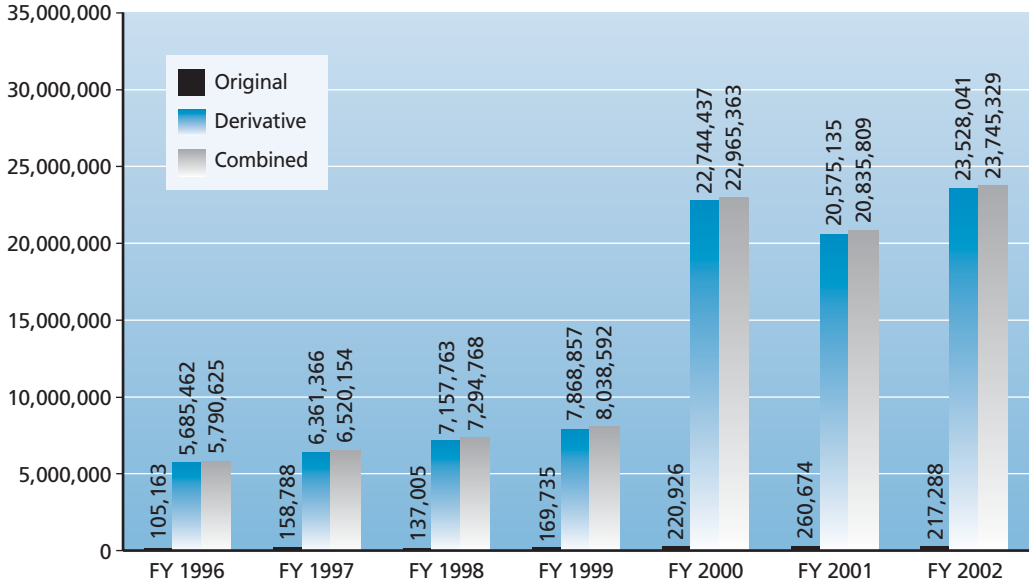


Combined Classification by Agency
Fiscal Year 2002



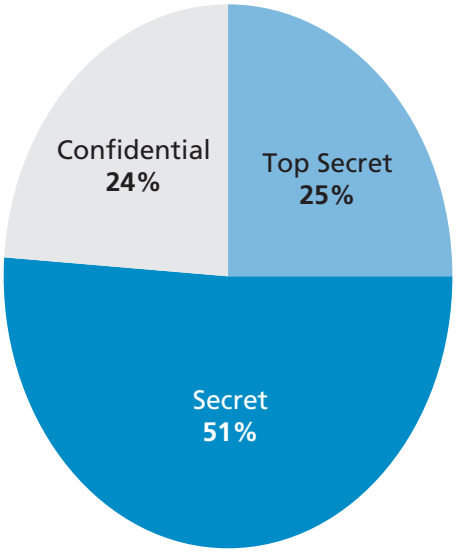
Original, Derivative and Combined Classification Activity

FY 1996-2002



Combined Classification by Level

Fiscal Year 2002



11 percent while Justice reported an increase of 39 percent.

With the uncertainty of world events at this time, ISOO cannot predict if there will be a continuing rise in classification activity in the coming years. We can only continue to monitor trends and encourage thoughtful and balanced decisions concerning the classification of information through ISOO's oversight activities.

Declassification

BACKGROUND

Declassification is an integral part of the security classification system. It is the authorized change in status of information from classified to unclassified. When

Executive Order 12958, was issued on April 17, 1995, the declassification policies of the past changed dramatically. In preceding years, classified information stayed classified and very often did not see the light of general public's, researchers' or historians' eyes without persistent and continuous efforts on the part of these individuals. E.O. 12958 changed this paradigm. With the Order's effective date of October 14, 1995, a new "Automatic Declassification" program was begun in addition to the longstanding "Systematic Review for Declassification".

Under the "Automatic Declassification" provision of E.O. 12958, information appraised as having permanent historical value is automatically declassified once it reaches 25 years of age unless an agency head has determined that it falls within a narrow exemption that permits continued classification. With the issuance of E.O. 12958, these records were subject to automatic declassification on April 17, 2000. Executive Order 13142, issued on November 19, 1999, amended E.O. 12958, to extend the date of the imposition of the automatic declassification provision until October 14, 2001. It also extended the date of the imposition of the automatic declassification provision an additional eighteen months, until April 17, 2003, for two groups of records, those that contain information classified by more than one agency and those that almost invariably contain information pertaining to intelligence sources or methods. While Executive branch agencies had made significant strides in trying to meet the April 17, 2003, deadline, it was clear in late 2001 that this latter deadline would not be met. Recognizing this, work was begun to further amend the Order to extend the deadline. On March 25, 2003, the signing of E.O. 13292 recommitted the executive branch to the automatic declassification process and extended the date of the imposition of the automatic declassification provision until December 31, 2006. By this date, executive branch agencies are expected to have either completed the declassification of their eligible records or properly exempted them.

"Systematic Review for Declassification," which began in 1972, is the program under which classified permanently valuable records are reviewed for the purpose of declassification after the records reach a specific age. Under E.O. 12356, the predecessor Order, the National Archives and Records Administration (NARA) was the only agency required to conduct a systematic review of its classified holdings.

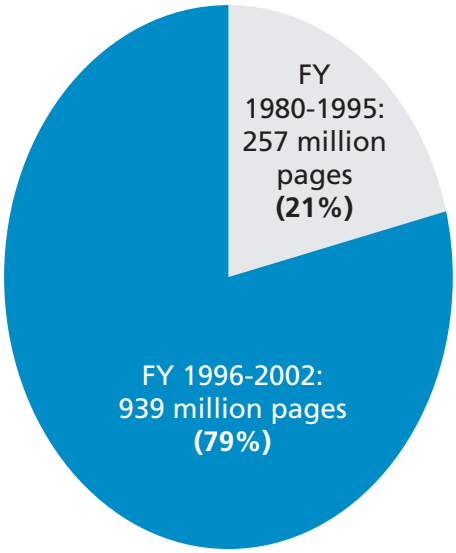
Now E.O. 12958 requires all agencies that originate classified information to establish and conduct a systematic declassification review program, which is undertaken in conjunction with the potential onset of automatic declassification. In effect, systematic review has become an appendage of the automatic declassification program. ISOO has collected data on declassification that does not distinguish between the two programs because they are now so interrelated.

In effect, E.O. 12958 reverses the resource burden. Unlike prior systems, in which agencies had to expend resources in order to declassify older information, under E.O. 12958, agencies must expend the resources necessary to demonstrate why older, historical information needs to remain classified. Fiscal year 2002 marked the seventh year in which the policies of the Order have been in effect.

PAGES DECLASSIFIED

During FY 2002, the executive branch declassified 44,365,711 pages of permanently valuable historical records. This figure represents a 56 percent decrease from that reported for FY 2001, and the largest decrease since Executive Order 12958 became effective on October 14, 1995. Even so, the number of pages declassified in FY 2002 continues to exceed the yearly average (12.6 million pages) under prior executive orders by three-fold. Given the many obstacles faced by executive branch agencies in their declassification efforts, this accomplishment is remarkable.

1.19 Billion Pages Declassified
Fiscal Year 1980-2002



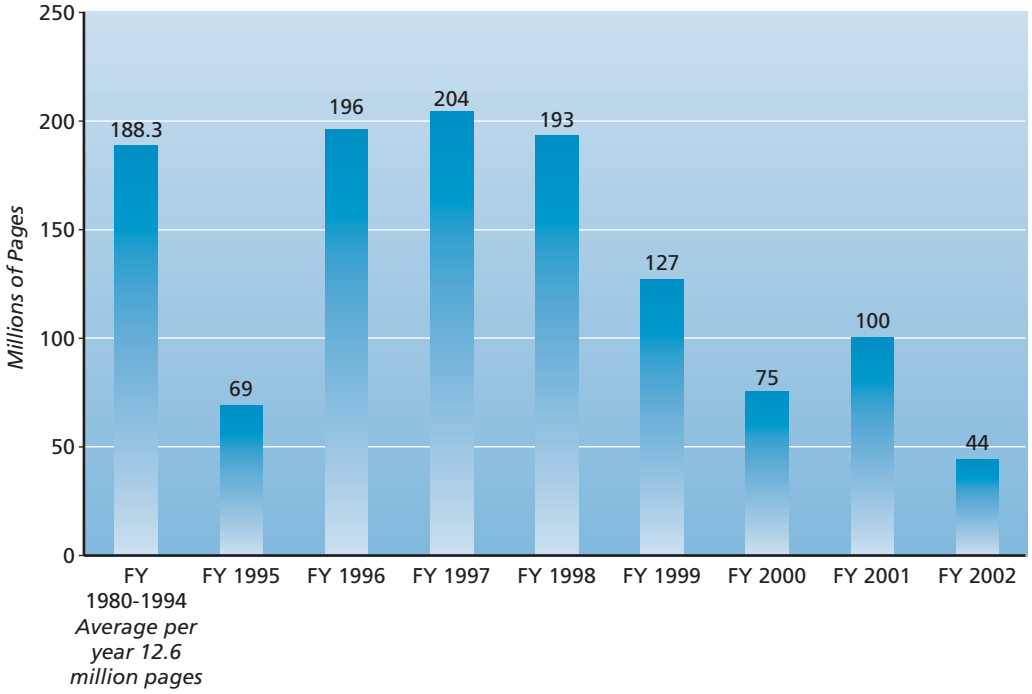
ISOO estimates that agencies have completed work on approximately 77 percent of the pages subject to automatic declassification, either by declassifying or exempting them. Those records remaining to be reviewed (an estimated 382 million pages based on the April 27, 2000, deadline) tend to be more complex and sensitive bodies of records dated 1976 and earlier. Such records require more time for review and processing. The number of pages subject to the automatic declassification provisions has not been updated since the November 1999 amendment to E.O. 12958. With the further amendment to E.O. 12958, in particular the automatic declassification provisions, ISOO will be asking agencies to again assess their records to determine the volume of records subject to this very important provision of the Order. This assessment will provide a better picture of the workload agencies will face to meet the final deadline set by the March 25, 2003 amendment to E.O. 12958.

Other factors outside the process have also affected declassification activity. The most significant factor has been the impact of the events of September 11, 2001. These events have caused agencies to look more closely at certain types of information before making declassification decisions. In particular, agencies are reviewing and re-reviewing

their records for information related to weapons of mass destruction and homeland security to ensure that the information contained in the records truly warrants continued protection. Legislation enacted in FY 1999 addressing the protection of Restricted Data and Formerly Restricted Data (Section 3161 of Public Law 105-261, entitled "Protection Against Inadvertent Release of Restricted Data and Formerly Restricted Data") and other special topical searches mandated by other legislative initiatives have required agencies to shift resources away from the automatic and systematic declassification programs to meet the requirements of the legislation. Additionally, as noted in the Security Cost Estimates section of this report, funding for declassification decreased by almost 50 percent, which we believe is also a result, at least in part, of the events of September 11th. It appears that funding has been shifted to other components of security, which is understandable. However, ISOO will closely monitor this aspect of agencies' declassification programs to ensure that this decrease in funding does not become permanent. Decreased funding will very clearly impact the ability of agencies to completely review their 25 year-old or older holdings prior to the deadline

1.19 Billion Pages Declassified

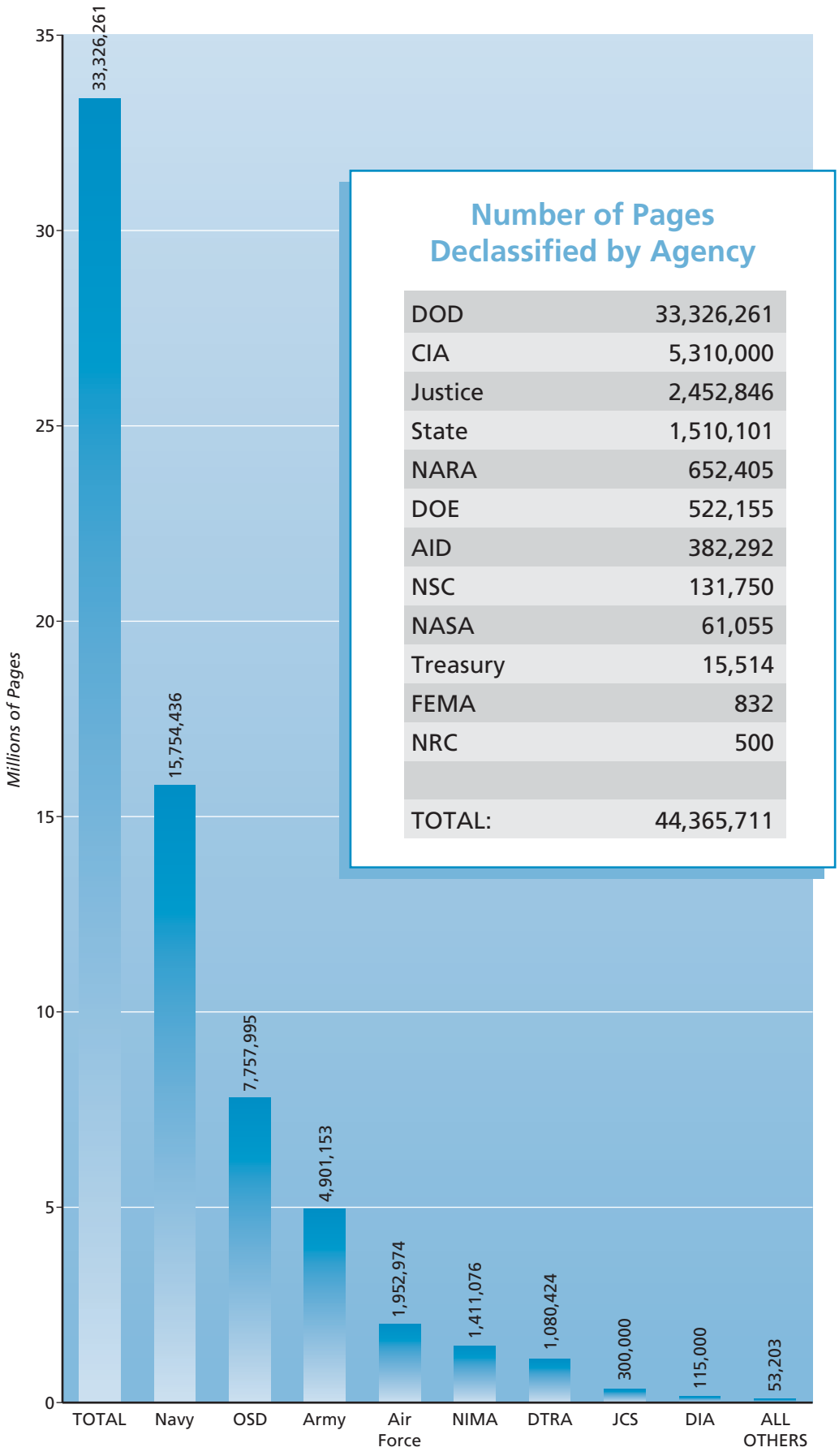
Fiscal Years 1980-2002



set for automatic declassification in the March 25, 2003 amendment to E.O. 12958. The consequence will be a shift back to the ever increasing "mountain" of classified records being stored in secure locations or containers across Government and contractor facilities.

The number of pages NARA declassified in FY 2002 again declined, from 3.2 million pages in FY 2001 to 652,405 pages in FY 2002. This is the lowest number of pages declassified by NARA since the first full year of implementation of the automatic declassification provisions of E.O. 12958 in 1996. Legislative mandates; page-by-page review requirements for NARA staff versus the use of sampling methods; and shifting staff resources to special reviews like "records of special interest—weapons of mass

DOD Components with Significant Numbers:



Number of Pages Declassified by Agency

DOD	33,326,261
CIA	5,310,000
Justice	2,452,846
State	1,510,101
NARA	652,405
DOE	522,155
AID	382,292
NSC	131,750
NASA	61,055
Treasury	15,514
FEMA	832
NRC	500
TOTAL:	44,365,711

destruction and homeland security related" all continue to contribute to NARA's decreased declassification activity.

Again, DOD led the executive branch in the number of total pages declassified in FY 2002, accounting for 75 percent of the total. While DOD led the executive branch, it, like NARA, reported the lowest number of pages declassified since the Order became effective on October 14, 1995.

Three agencies reported remarkable increases in their declassification activity during FY 2002 as compared to FY 2001: NSC (476%); State (242%); and Justice (41%). Those agencies that experienced significant decreases include: Treasury (82%); NASA (58%); AID (52%); FEMA (36%); CIA (25%); and DOE (16%). ISOO encourages all these agencies to sustain or work to increase their efforts to implement their automatic declassification programs.

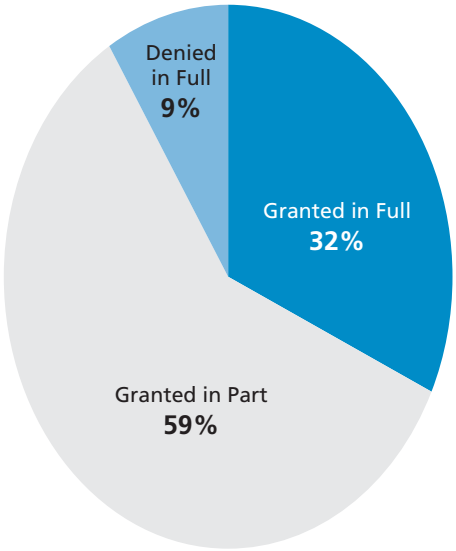
In the seven years that Executive Order 12958 has been in effect, executive branch agencies have declassified over 939 million pages of permanently valuable historical records. Compared to the 257 million pages declassified under the prior two executive orders (E.O. 12065 and E.O. 12356) and before E.O. 12958 became effective, the executive branch in the past seven years has more than tripled the number of pages declassified. Since ISOO came into existence in late 1978, and began collecting and analyzing data beginning in FY 1980, it has reported the declassification of permanently valuable records totaling approximately 1.2 billion pages. Of that total, 1 billion pages or 84 percent, have been declassified due in large part to the automatic declassification provision of E.O. 12958.

LOOKING AHEAD

The data reported by agencies about their automatic declassification programs clearly show that our changed security environment has had an impact. Agencies have reconsidered the declassification of certain types of information, like weapons of mass destruction. With declassification infrastructures in place as a result of the declassification policies contained in this Order, agencies were better able to address these records of concern than they were before the automatic declassification program was instituted in 1995. While declassification cost estimates went down in fiscal year 2002 (see Security Cost Estimates section of this Report), it is to the benefit of the executive branch and the public to ensure that this does not become a trend. As the executive branch looks forward to a new deadline for automatic declassification, it must prepare for the challenges that this new deadline brings, which includes continued funding and support. ISOO, in concert with the agencies, will need to find new process improvements to

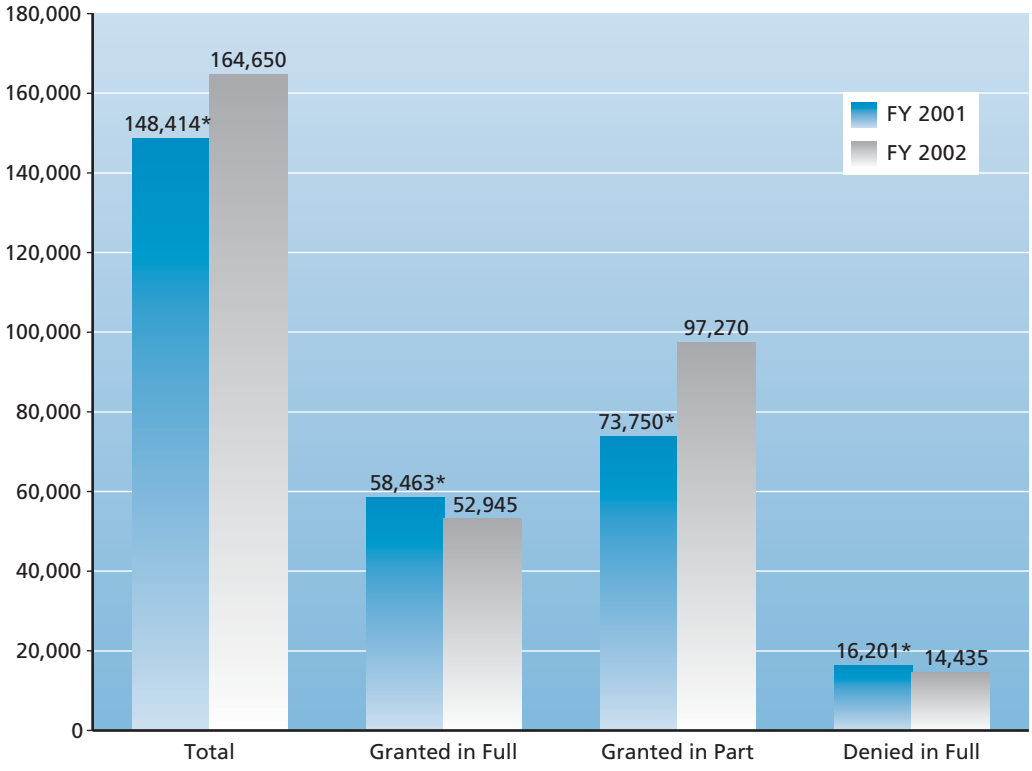
Mandatory Review Appeals Disposition

Fiscal Year 2002



Mandatory Review Pages Processed

Fiscal Years 2001-2002



*Data for FY 2001 reflect revised figures for DOD.

meet the December 31, 2006 deadline. This will require cooperation, innovative thinking and hard work, which will in the end, benefit, not only the general public, historians and researchers, but also the agencies. Knowing, understanding and managing the information contained in agencies' records systems is an essential part of the overall solution. Technology is ever moving us forward and will also be an important element in the solution. We must push the envelope and recognize the future of information in the electronic environment. It is the challenge of the information age.

MANDATORY REVIEW

Under Executive Order 12958, the mandatory review process permits individuals or agencies 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 presidential papers or records, which are not subject to the FOIA.

During FY 2002, agencies processed 3,284 cases, totaling 164,650 pages. The number of pages processed increased by 11 percent from the previous year. Both the number of pages and the percentage of pages declassified in whole or in part

increased, from 132,213 pages and 89 percent to 150,215 pages and 91 percent. The percentage of pages declassified in whole or in part has remained high under Executive Order 12958, with this year's rate being the third highest of the last seven years. While outside factors, such as our new security environment, and special search legislation, have had an impact on how many mandatory declassification review requests can be processed by the agencies, ISOO believes that mandatory review remains a very successful means for declassifying information.

During FY 2002, agencies processed 84 appeals that comprised 5,327 pages. Of these, 83 percent of the pages were granted in whole or in part. The rate is 34 percent higher than last year and is the third highest rate since this Order became effective on October 14, 1995. The higher rate of declassification suggests that researchers can continue to anticipate greater return in declassified information if they pursue an appeal.

Agency Acronyms or Abbreviations

AID:	Agency for International Development
Air Force:	Department of the Air Force
Army:	Department of the Army
CEA:	Council of Economic Advisers
CIA:	Central Intelligence Agency
Commerce:	Department of Commerce
DARPA:	Defense Advanced Research Projects Agency
DCAA:	Defense Contract Audit Agency
DIA:	Defense Intelligence Agency
DISA:	Defense Information Systems Agency
DLA:	Defense Logistics Agency
DOD:	Department of Defense
DOE:	Department of Energy
DOT:	Department of Transportation
DSS:	Defense Security Service
DTRA:	Defense Threat Reduction Agency
ED:	Department of Education
EPA:	Environmental Protection Agency
EXIMBANK:	Export-Import Bank
FBI:	Federal Bureau of Investigation
FCC:	Federal Communications Commission
FEMA:	Federal Emergency Management Agency
FMC:	Federal Maritime Commission
FRS:	Federal Reserve System
GSA:	General Services Administration
HHS:	Department of Health and Human Services
HUD:	Department of Housing and Urban Development
Interior:	Department of the Interior
ISCAP:	Interagency Security Classification Appeals Panel
ISOO:	Information Security Oversight Office
ITC:	International Trade Commission
JCS:	Joint Chiefs of Staff
Justice:	Department of Justice
Labor:	Department of Labor
MMC:	Marine Mammal Commission
MSPB:	Merit Systems Protection Board
MDA:	Missile Defense Agency
NARA:	National Archives and Records Administration
NASA:	National Aeronautics and Space Administration
Navy:	Department of the Navy
NISPPAC:	National Industrial Security Program Policy Advisory Committee
NIMA:	National Imagery and Mapping Agency
NRC:	Nuclear Regulatory Commission
NRO:	National Reconnaissance Office
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
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
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

The National Archives Building
Seventh & Pennsylvania Avenue, NW
Washington, DC 20408

Telephone: 202.219.5250
Fax: 202.219.5385
Email: isoo@nara.gov
Web site: www.archives.gov/isoo/index.html

FROM THE

Federal Register

VOL. 68, NO. 60,

FRIDAY, MARCH 28, 2003

PART III

The President

Executive Order 13292

Further Amendment to Executive Order 12958, as Amended,

Classified National Security Information

Executive Order 13292—Further Amendment to Executive Order 12958, as Amended, Classified National Security Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to further amend Executive Order 12958, as amended, it is hereby ordered that Executive Order 12958 is amended to read as follows:

Classified National Security Information

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. 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 defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security remains a priority.

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. *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 1.4 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, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

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

(c) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

Sec. 1.2. *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.

Sec. 1.3. *Classification Authority.* (a) The authority to classify information originally may be exercised only by:

(1) the President and, in the performance of executive duties, the Vice President;

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

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

(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; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) ''Secret'' or ''Confidential'' original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section; or the senior agency official described in section 5.4(d) of this order, 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. Such training must include instruction on the proper safeguarding of classified information and of the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure.

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

Sec. 1.4. *Classification Categories.* Information shall 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, which includes defense against transnational terrorism;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

(h) weapons of mass destruction.

Sec. 1.5. *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. Upon reaching the date or event, the information shall be automatically declassified. The date or event shall not exceed the time frame established in paragraph (b) of this section.

(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, unless the original classification authority otherwise determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years from the date of the original decision. All information classified under this section shall be subject to section 3.3 of this order if it is contained in records of permanent historical value under title 44, United States Code.

(c) An original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) Information marked for an indefinite duration of classification under predecessor orders, for example, marked as ''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. 1.6. *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 1.2 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 1.5(a) or section 1.5(c);

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b); or

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5 (b); and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information described in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, 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. 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. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(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.

(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

Sec. 1.7. *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 the national security.

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

(c) Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions:

(1) the reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of the national security;

(2) the information may be reasonably recovered; and

(3) the reclassification action is reported promptly to the Director of the Information Security Oversight Office.

(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 3.5 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 5.4 of this order.

(e) Compilations of items of information that 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. 1.8. *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) of this section.

(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 ensure 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 (Panel) established by section 5.3 of this order.

PART 2—DERIVATIVE CLASSIFICATION

Sec. 2.1. *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. 2.2. *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 ensure that classification guides are reviewed and updated as provided in directives issued under this order.

PART 3—DECLASSIFICATION AND DOWNGRADING

Sec. 3.1. *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 the 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. 3.2. *Transferred Records.* (a) In the case of classified records 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 records that are not officially transferred as described in paragraph (a) of this section, 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 records shall be deemed to be the originating agency for purposes of this order. Such records 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 records.

(c) Classified records 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 of the United States (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 classified records be accessioned into the National

Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone 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 section 3.3 of this order.

Sec. 3.3. *Automatic Declassification*. (a) Subject to paragraphs (b)–(e) of this section, on December 31, 2006, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of its original classification, except as provided in paragraphs (b)–(e) of this section.

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

(1) reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

(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, including foreign government 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 protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

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

(c) 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 that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section 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) of this section, 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. File series exemptions previously approved by the President shall remain valid without any additional agency action.

(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 Panel, of any specific information beyond that included in a notification to the President under paragraph (c) of this section that the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the information, either by reference to information in specific records or in the form of a declassification guide;

(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) of this section, 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) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 5 additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly.

(3) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years for classified records that have been referred or transferred to that agency by another agency less than 3 years before automatic declassification would otherwise be required.

(4) By notification to the Director of the Information Security Oversight Office, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of 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.

(h) Records containing information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies shall be referred for review to those agencies and the information of concern shall be subject to automatic declassification only by those agencies, consistent with the provisions of subparagraphs (e)(3) and (e)(4) of this section.

Sec. 3.4. *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 records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize the systematic review of records based upon the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist shall conduct a systematic declassification review program for classified records: (1) accessioned into the National Archives as of the effective date of this order; (2) transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) for which the National Archives serves as the custodian for 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 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 ensure 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. 3.5. *Mandatory Declassification Review.* (a) Except as provided in paragraph (b) of this section, 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 sections 105C, 105D, or 701 of the National Security Act of 1947 (50 U.S.C. 403– 5c, 403–5e, and 431); and

(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by:

(1) the incumbent President or, in the performance of executive duties, the incumbent Vice President;

(2) the incumbent President's White House Staff or, in the performance of executive duties, the incumbent Vice President's 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) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records 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 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 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. 3.6. *Processing Requests and Reviews.* In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

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

(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 or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.7. *Declassification Database.* (a) The Director of the Information Security Oversight Office, in conjunction with those agencies that originate classified information, shall coordinate the linkage and effective utilization of existing agency databases of records that have been declassified and publicly released.

(b) Agency heads shall fully cooperate with the Director of the Information Security Oversight Office in these efforts.

PART 4—SAFEGUARDING

Sec. 4.1. *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) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) 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.

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

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

(f) 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.

(g) 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.

(h) 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 modified handling and transmission and 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.

(i) Except as otherwise provided by statute, this order, directives implementing this order, or by direction of the President, classified information originating in one agency shall 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. Prior consent is not required when referring records for declassification review that contain information originating in several agencies.

Sec. 4.2. *Distribution Controls.* (a) Each agency shall establish controls over the distribution of classified information to ensure that it is distributed only to organizations or individuals eligible for access and with a need-to-know the information.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with the directives implementing this order and any procedures issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of

Central Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

(c) 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. 4.3. *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 shall 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 when the program is required by statute or 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.

(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 5.4(d) 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 head shall brief the Assistant to the President for National Security Affairs, or a designee, on any or all of the agency's special access programs.

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

Sec. 4.4. *Access by Historical Researchers and Certain Former Government Personnel.* (a) The requirement in section 4.1(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;

(2) previously have occupied policy-making positions to which they were appointed by the President under section 105(a)(2)(A) of title 3, United States Code, or the Vice President under 106(a)(1)(A) of title 3, United States Code; or

(3) served as President or Vice 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 the 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 and Vice Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee or a Vice Presidential appointee.

PART 5—IMPLEMENTATION AND REVIEW

Sec. 5.1. *Program Direction*. (a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the Assistant to the President for National Security Affairs, 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 Information Security Oversight Office shall establish standards for:

(1) classification and marking principles;

(2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;

(3) agency security education and training programs;

(4) agency self-inspection programs; and

(5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

Sec. 5.2. *Information Security Oversight Office*. (a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, 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 President through the Assistant to the President for National Security Affairs within 60 days of the request for access. Access shall be denied pending the response;

(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 Assistant to the President for National Security Affairs;

(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. 5.3. *Interagency Security Classification Appeals Panel.*

(a) Establishment and administration.

(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the Central Intelligence Agency, the National Archives, and the Assistant to the President for National Security Affairs shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. 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 (a)(1) of this section.

(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 1.8 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order.

(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the **Federal Register**. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

(2) there is no current action pending on the issue within the Federal courts; and

(3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

(d) Agency heads shall 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 shall 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 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 changed by the President.

(f) Notwithstanding paragraphs (a) through (e) of this section, whenever the Panel reaches a conclusion that information owned or controlled by the Director of Central Intelligence (Director) should be declassified, and the Director notifies the Panel that he objects to its conclusion because he has determined that the information could reasonably be expected to cause damage to the national security and to reveal (1) the identity of a human intelligence source, or (2) information about the application of an intelligence source or method (including any information that concerns, or is provided as a result of, a relationship with a cooperating intelligence element of a foreign government), the information shall remain classified unless the Director's determination is appealed to the President, and the President reverses the determination.

Sec. 5.4. *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) ensure that agency records systems are designed and maintained to optimize the safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

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

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

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

(3) establishing and maintaining security education and training programs;

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

(5) establishing procedures to prevent unnecessary access to classified information, including procedures that:

(A) require that a need for access to classified information is established before initiating administrative clearance procedures; and

(B) 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) ensuring 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:

(A) original classification authorities;

(B) security managers or security specialists; and

(C) 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. 5.5. *Sanctions.* (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has 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) of this section occurs; and

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

PART 6—GENERAL PROVISIONS

Sec. 6.1. *Definitions.* For purposes of this order:

(a) ''Access'' means the ability or opportunity to gain knowledge of classified information.

(b) ''Agency'' means any ''Executive agency,'' as defined in 5 U.S.C. 105; any ''Military department'' as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) ''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.

(d) ''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.

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

(f) ''Classification guidance'' means any instruction or source that prescribes the classification of specific information.

(g) ''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.

(h) ''Classified national security information'' or ''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.

(i) ''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.

(j) ''Damage to the national security'' means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(k) ''Declassification'' means the authorized change in the status of information from classified information to unclassified information.

(l) ''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.

(m) ''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.

(n) ''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.

(o) ''Document'' means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(p) ''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.

(q) ''File series'' means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(r) ''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 Government 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.

(s) ''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.

(t) ''Infraction'' means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a ''violation,'' as defined below.

(u) ''Integral file block'' means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time such as presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group.

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

(w) ''Mandatory declassification review'' means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

(x) ''Multiple sources'' means two or more source documents, classification guides, or a combination of both.

(y) ''National security'' means the national defense or foreign relations of the United States.

(z) ''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.

(aa) ''Network'' means a system of two or more computers that can exchange data or information.

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

(cc) ''Original classification authority'' means an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.

(dd) ''Records'' means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ee) ''Records having permanent historical value'' means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(ff) ''Records management'' means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(gg) ''Safeguarding'' means measures and controls that are prescribed to protect classified information.

(hh) ''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.

(ii) ''Senior agency official'' means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

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

(kk) ''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.

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

(mm) ''Telecommunications'' means the preparation, transmission, or communication of information by electronic means.

(nn) ''Unauthorized disclosure'' means a communication or physical transfer of classified information to an unauthorized recipient.

(oo) ''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.

(pp) ''Weapons of mass destruction'' means chemical, biological, radiological, and nuclear weapons.

Sec. 6.2. *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 Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, officers, employees, or agents. The foregoing is in addition to the specific provisos set forth in sections 3.1(b) and 5.3(e) of this order.''

(d) Executive Order 12356 of April 6, 1982, was revoked as of October 14, 1995.

Sec. 6.3. *Effective Date.* This order is effective immediately, except for section 1.6, which shall become effective 180 days from the date of this order.

THE WHITE HOUSE,
March 25, 2003.