2004

INFORMATION SECURITY OVERSIGHT OFFICE • **REPORT TO THE PRESIDENT**

REPORT TO THE PRESIDENT 2004

INFORMATION SECURITY OVERSIGHT OFFICE

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).
- Provides program and administrative support for the Public Interest Declassification Board (PIDB).
- Reviews requests for original classification authority from agencies.
- Chairs interagency meetings to discuss matters pertaining to both Orders.
- Reviews and approves agency implementing regulations and agency guides for systematic declassification review.

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.
- Provide expert advice and guidance pertinent to the principles of information security.

AUTHORITY

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

March 31, 2005

The President
The White House
Washington, DC 20500

Dear Mr. President:

We are pleased to submit to you the 2004 Report of the Information Security Oversight Office (ISOO).

This report provides information on the status of the security classification program as required by Executive Order 12958, as amended, "Classified National Security Information." It includes statistics and analysis concerning components of the system, primarily classification, declassification, and the ISOO inspection program. It also contains information with respect to industrial security in the private sector as required by Executive Order 12829, as amended, "National Industrial Security Program."

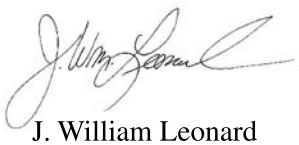
One of the most notable developments of the year occurred when the National Industrial Security Program Policy Advisory Committee approved a "Declaration of Principles for Reciprocity of Access Eligibility Determinations Within Industry." Provided this declaration is uniformly implemented, it will provide some relief to the current personnel security clearance crisis within industry.

Also of note was your appointment of members to the Public Interest Declassification Board. This Board will contribute to the declassification of records on specific subjects that are of extraordinary public interest where it is deemed that declassification will not undermine the national security interests of the United States.

In addition, ISOO focused on evaluating Executive branch progress toward the orderly declassification of historically valuable permanent classified records that are 25-years-old or older. For the most part, the Executive branch is progressing well toward the deadline of December 31, 2006. Nonetheless, a significant number of agencies remain at risk of falling short. ISOO will continue its vigorous effort to evaluate, advise, and assist all pertinent agencies, with a view toward fulfilling the commitment to the deadline.

A responsible security classification system and a committed declassification program are the cornerstones of an open and efficient government that serves both to protect and to inform its citizens. Ensuring that these cornerstones are properly placed requires diligence and integrity in regard to the American ideals of providing for our national security within the context of a free and open society.

Respectfully,



J. William Leonard
Director

TABLE OF CONTENTS

NOTE: The Report on Cost Estimates for Security Classification Activities will be reported separately.

SUMMARY OF FISCAL YEAR 2004 PROGRAM ACTIVITY

The following Report to the President is the ninth report under E.O. 12958, which went into effect in October 1995 and was amended on March 25, 2003. The following data highlight ISOO's findings.

Classification

- Executive branch agencies reported 4,007 original classification authorities.
- Agencies reported 351,150 original classification decisions.
- Executive branch agencies reported 15,294,087 derivative classification decisions.
- Agencies reported 15,645,237 combined classification decisions.

Declassification

- Under Automatic and Systematic Review Declassification programs, agencies declassified 28,413,690 pages of historically valuable records.
- Agencies processed 4,470 new mandatory review requests.
- Under mandatory review, agencies declassified in full 224,342 pages; declassified in part 64,443 pages; and retained classification in full on 15,590 pages.
- Agencies received 163 new mandatory review appeals.
- On appeal, agencies declassified in whole or in part 3,889 additional pages.

GETTING IT RIGHT

The system for classifying national security information has consistently been criticized as replete with overclassification. Often, this report and its reference to the steadily increasing number of overall classification decisions from year to year is cited as an indicator that overclassification persists within the executive branch. It must be noted that during the period from fiscal year 2002 through fiscal year 2004, the U.S. Government built a new structure for homeland security and engaged in wars in Afghanistan and Iraq and against al-Qaeda. At the same time, information technology has exponentially increased the Government's ability to produce information of all sorts, both classified and unclassified. It cannot be said conclusively from this report's data that recent increases in the number of classification decisions were due substantially to the phenomenon of "overclassification." Is it simply a reflection of an increase in legitimate classification decisions as a result of the upsurge in the tempo of national security operations? Overclassification has been a consistent issue over the past several decades. This matter has been highlighted in far-reaching reviews such as those by the Commission on Government Security in 1955, the Department of Defense Security Review Commission in 1985, and the Commission on Protecting and Reducing Government Secrecy in 1997, and in nearly every other study on this issue.

The system for classifying national security information is an essential and proven tool for defending our nation. The ability to surprise and deceive the enemy can spell the difference between success and failure on the battlefield. Similarly, it is nearly impossible for our intelligence services to recruit human sources (who often risk their lives aiding our country) or to obtain assistance from other countries' intelligence services unless such sources can be assured complete and total confidentiality. Likewise, certain intelligence methods can work only if the adversary is unaware of their existence. Finally, the successful discourse between nations often depends on constructive ambiguity and plausible deniability as the only way to balance competing and divergent national interests.

Classification, of course, can be a double-edged sword. Limitations on dissemination of information that are designed to deny information to the enemy on the battlefield can increase the risk that our own forces will be unaware of important information, contributing to the potential for friendly fire incidents or other failures. Likewise, imposing strict compartmentalization of information obtained from human agents increases the risk that a Government official with access to other information that could cast doubt on the reliability of the agent would not know of the use of that agent's information elsewhere in the Government. The National Commission on Terrorist Attacks Upon the United States noted that while it could not state for certain that the sharing of information would have succeeded in disrupting the 9/11 plot, it could state that the failure to share information contributed to the government's failure to interrupt the plot. Simply put, secrecy comes at a price. For classification to work, agency officials must become more successful in factoring this reality into the overall risk equation when making classification decisions.

Classification is an important fundamental principle when it comes to national security, but it need not and should not be an automatic first principle. In certain circumstances, even with respect to national security information, classification can run counter to our national interest. The decision to classify information or not is ultimately the prerogative of the original classification authorities (OCAs) in each agency. The exercise of an OCA's prerogative to classify certain information has ripple effects throughout the entire executive branch. For example, it can serve as an impediment to sharing information with those who genuinely need to know this information; another agency, state or local officials, or the public.

The approximately 4,000 officials with original classification authority play a critical role in ensuring the effectiveness and the overall integrity of the classification system. Because they are the only individuals in the process authorized to exercise discretion in making classification decisions, their decision to classify particular information constitutes the first stage in the life cycle of classified national security information and can spawn hundreds if not thousands of derivative classification decisions. At a minimum, for each original classification decision, original classification authorities need to be able to identify or describe the damage to national security that would reasonably arise if the information were subject to unauthorized disclosure. To ensure that the original classification decision is necessary, original classification authorities should also be able to describe how the information differs from information already classified. To this end, original classification authorities should consult existing classification guidance to ensure that the information is not already classified.

While original classification authorities play a critical role in the first step of classification, it is derivative classifiers who make 92 percent of all classification decisions. They do this when they extract or paraphrase information in already classified materials or use their own interpretation of what they believe requires classification when consulting overly generalized classification guides. What derivative classifiers must always be mindful of is that they must be able to trace the origins of every act of derivatively classifying information to an explicit decision by a responsible official who has been expressly delegated original classification authority.

The single most significant step agencies can take in enhancing the integrity and effectiveness of the classification system for national security information is to enhance the quality of classification guides. The specificity as to what information is classified, at what level, and for what duration is the foundation of the system. Guides must also be reviewed frequently and updated at least once every five years, and those that contradict one another must be reconciled. Most important of all, derivative classifiers must be trained so that they have a clear understanding of the guides, and agencies must ensure that they are appropriately implementing original classification decisions.

Overclassification, besides needlessly and perhaps dangerously restricting information sharing, also wastes untold dollars. One of the most effective steps agencies can take to address these concerns is to ensure that classification becomes an informed, deliberate decision rather than one committed by rote. In the final analysis, it is the people who deal with the information, their knowledge and understanding of the program, and their faith in the integrity of the classification system that protects truly sensitive national security information from unauthorized disclosure. This knowledge, understanding, and confidence cannot be taken for granted; it requires clear, forceful and continuous effort by senior leadership to make it happen. The consequences of failure are too high. The American people expect and deserve nothing less than that we make the right classification decisions each and every day.

INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

AUTHORITY

Section 5.3 of Executive Order 12958, as amended, "Classified National Security Information."

FUNCTIONS

- Decides on appeals by authorized persons who have filed classification challenges under section 1.8 of E.O. 12958, as amended.
- Approves, denies, or amends agency exemptions from automatic declassification as provided in section 3.3 of E.O. 12958, as amended.
- Decides on appeals by persons or entities who have filed requests for mandatory declassification review (MDR) under section 3.5 of E.O. 12958, as amended.

MEMBERS

William H. Leary, Chair
National Security Council

James A. Baker
Department of Justice

Edmund Cohen
Central Intelligence Agency

Margaret P. Grafeld
Department of State

Carol A. Haave
Department of Defense

Michael J. Kurtz
National Archives and Records Administration

EXECUTIVE SECRETARY

J. William Leonard, Director
Information Security Oversight Office

SUPPORT STAFF

Information Security Oversight Office

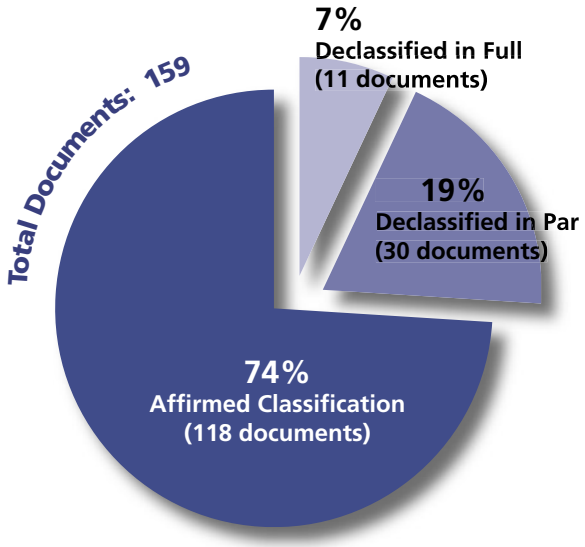
SUMMARY OF ACTIVITY

The Interagency Security Classification Appeals Panel (ISCAP) was created under E.O. 12958 to perform the critical functions noted above. The ISCAP, composed of senior-level representatives appointed by the Secretaries of State and Defense, the Attorney General, the Director of the Central Intelligence Agency, the Archivist of the United States, and the Assistant to the President for National Security Affairs, began meeting in May 1996. The President selects its Chair, the Director of the Information Security Oversight Office (ISOO) serves as its Executive Secretary, and ISOO provides its staff support.

To date, the majority of the ISCAP's efforts have focused on MDR appeals. During fiscal year 2004, the ISCAP decided on 159 documents that remained fully or partially classified on the completion of agency processing. It declassified information in 26 percent of the documents that it decided on; declassifying the entirety of the remaining classified information in 11 documents (7 percent) and declassifying some portions while affirming the classification of other portions in 30 of the documents (19 percent). The ISCAP fully affirmed the prior agency decisions in their entirety for 118 documents (74 percent).

It should be noted that during fiscal year 2004, a majority of the 159 documents reviewed by the ISCAP were less than 25 years old. As such, they were subject to a broader standard for classification than that used for information that is more than 25 years old (see section 1.4 as compared to section 3.3(b) of the amended Order). Given the much lower threshold for classification of information that is less than 25 years old, the shift to a higher percentage of agency decisions affirmed in part or in their entirety by the ISCAP is not surprising.

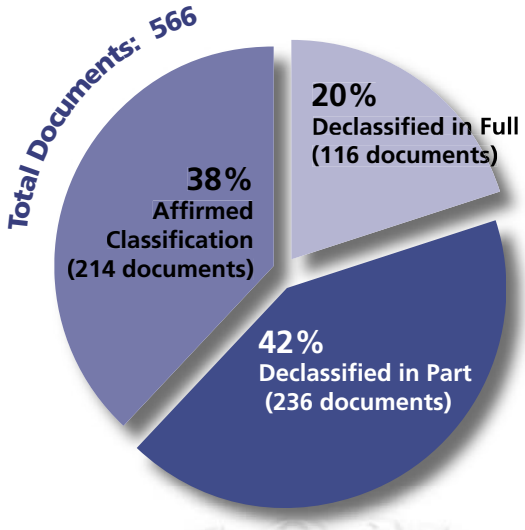
From May 1996 through September 2004, the ISCAP decided on 566 documents. The ISCAP declassified information in 62 percent of these documents. Specifically, it declassified the entirety of the remaining classified information in 116 documents (20 percent) and declassified some portions while affirming the classification of other portions in 236 documents (42 percent). The ISCAP fully affirmed agency classification decisions in 214 documents (38 percent).



ISCAP Decisions
Fiscal Year 2004

While the chart to the right depicts an increase over time in the percentage of agency decisions affirmed in part or in their entirety by the ISCAP, the shift is the result of a number of factors. For example, the age of the information in individual appeals can have an impact on the ISCAP's decisions. Moreover, there is the normal maturation of the standards and principles of E.O. 12958, as amended, throughout the Executive branch. As agencies gain experience with the provisions of the amended Order, the ISCAP has seen less misapplication of the classification standards. Furthermore, although its decisions are not intended to be precedent-setting, the impact of the ISCAP on agency positions relative to MDRs is apparent. As set forth elsewhere in this report, MDRs by agencies result in the declassification, in whole or in part, of more than 91 percent of the pages reviewed. Even after such thoughtful and thorough reviews by agencies, the ISCAP declassification of additional information in 62 percent of the appeals filed is significant.

Documents declassified by the ISCAP may be requested from the entity that has custody of them, usually a presidential library. For assistance in identifying and requesting copies of such documents, please contact the ISCAP staff at ISOO.



ISCAP Decisions
May 1996-September 2004

APPEALS CONCERNING ISCAP DECISIONS

In recognition of the need to hear appeals of agency decisions relating to the MDR program and of the reality that hearing such appeals would be an undue burden on the President, E.O. 12958 established the ISCAP to advise and assist the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Whereas the ISCAP exercises Presidential discretion in its decisions, it serves as the highest appellate authority for MDR appeals.

The ISCAP's decisions are committed to the discretion of the Panel, unless changed by the President. Since its original issuance in 1995, E.O. 12958 has provided agency heads with the ability to appeal the ISCAP's decisions to the President through the Assistant to the President for National Security Affairs. From May 1996 through the amendment of E.O. 12958 in fiscal year 2003, this authority had not been exercised by any agency head; the same was true for fiscal year 2004.

However, the amendment of the Order in fiscal year 2003 allows the Director of Central Intelligence (DCI) to object to the declassification by the ISCAP of certain information owned or controlled by the DCI. Such determinations by the DCI may be appealed to the President (see section 5.3(f) of the amended Order). The information remains classified unless the President reverses the DCI's determination.

In the latter part of fiscal year 2003, the DCI objected to the declassification of two documents that the ISCAP had voted to declassify. In both instances, in early fiscal year 2004, individual members of the ISCAP appealed the DCI's determination to the President through the Assistant to the President for National Security Affairs. During that fiscal year, one of these appeals was rendered moot when the DCI later exercised his discretion and declassified the document at issue in its entirety. As of the end of fiscal year 2004, the second appeal remains pending, and thus the document remains classified in its entirety.

During fiscal year 2004, a year in which the ISCAP decided on its largest number of documents to date, the DCI did not object under section 5.3(f) of the amended Order to the declassification of any information.

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

Telephone: 202.219.5250

Fax: 202.219.5385

Email: iscap@nara.gov

Additional information about ISCAP may be found on this portion of the ISOO website:

www.archives.gov/isoo/oversight_groups/iscap/iscap.html

NATIONAL INDUSTRIAL SECURITY PROGRAM

In fiscal year 2004, a Government and industry National Industrial Security Program Policy Advisory Committee (NISPPAC) approved by consensus a "Declaration of Principles" with respect to reciprocity of security clearances within industry. This declaration represents a clear articulation of what reciprocity is (and is not) with enough specificity and substance that industry can hold Government agencies accountable for their actions in this area. While it should provide some relief to the current personnel security clearance crisis within industry, it is not a silver bullet. However, it provides a Government point of contact for industry to report practices contrary to the principles of reciprocity.

On August 6, 2004, this Declaration of Principles was formally promulgated and forwarded to the Secretary of Defense, the Secretary of Energy, the Acting Director, Central Intelligence Agency, and the Chairman of the Nuclear Regulatory Commission for immediate implementation, to include designation of an appropriate point of contact as well as dissemination to their cleared contractors. A copy has also been sent to the Assistant to the President for National Security Affairs for forwarding to the Records Access and Information Security Policy Coordinating Committee under the National Security Council (NSC) for the development of any additional interagency implementing processes.

This Declaration of Principles is reprinted in this report under Appendix A.

During fiscal year 2004, ISOO formulated an implementing directive to the National Industrial Security Program (NISP) Order. The implementing directive provides additional direction to assist agencies in their implementation of the NISP. The implementing directive has been forwarded to the NSC pending final approval.

CLASSIFICATION

OVERVIEW

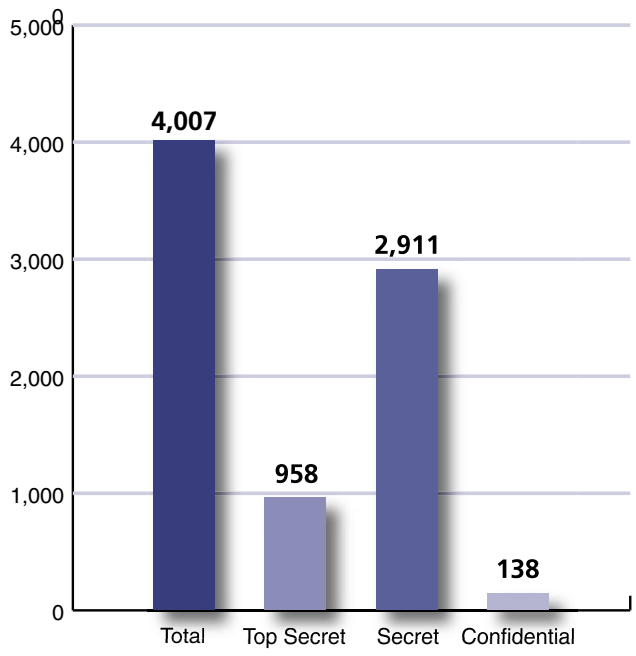
The level of classification activity in fiscal year 2004 continues to be driven by events, policies, and programs instituted in the aftermath of the major terrorist attacks perpetrated against the United States in 2001. New entities within the federal executive branch, such as the Department of Homeland Security (DHS), are still developing, and counterterrorism analysis and operations continue to be a major emphasis. The continuing increase in classification activity appears to be driven mainly by the ongoing war on terror and the military operations in Iraq and Afghanistan. Fiscal year 2004 also marks the first full fiscal year of military operations in Iraq.

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, as amended, 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.

There was little net change in the number of OCAs during fiscal year 2004. Several large agencies have achieved success in their efforts to reduce their number of OCAs. Most notable of these were the Department of Commerce (Commerce), the Department of Energy (DOE), the Department of Transportation (DOT), and the Department of the Treasury (Treasury). These agencies reported decreases of 15 percent, 6 percent, 30 percent, and 64 percent, respectively. On the other hand, DHS increased from 18 to 83 OCAs. DHS is still rounding out its senior positions and receiving positions that previously resided in other agencies, including DOT and Treasury. The net effect was an increase from 3,978 to 4,007, or 1 percent, in the number of officials with original classification authority.[1]

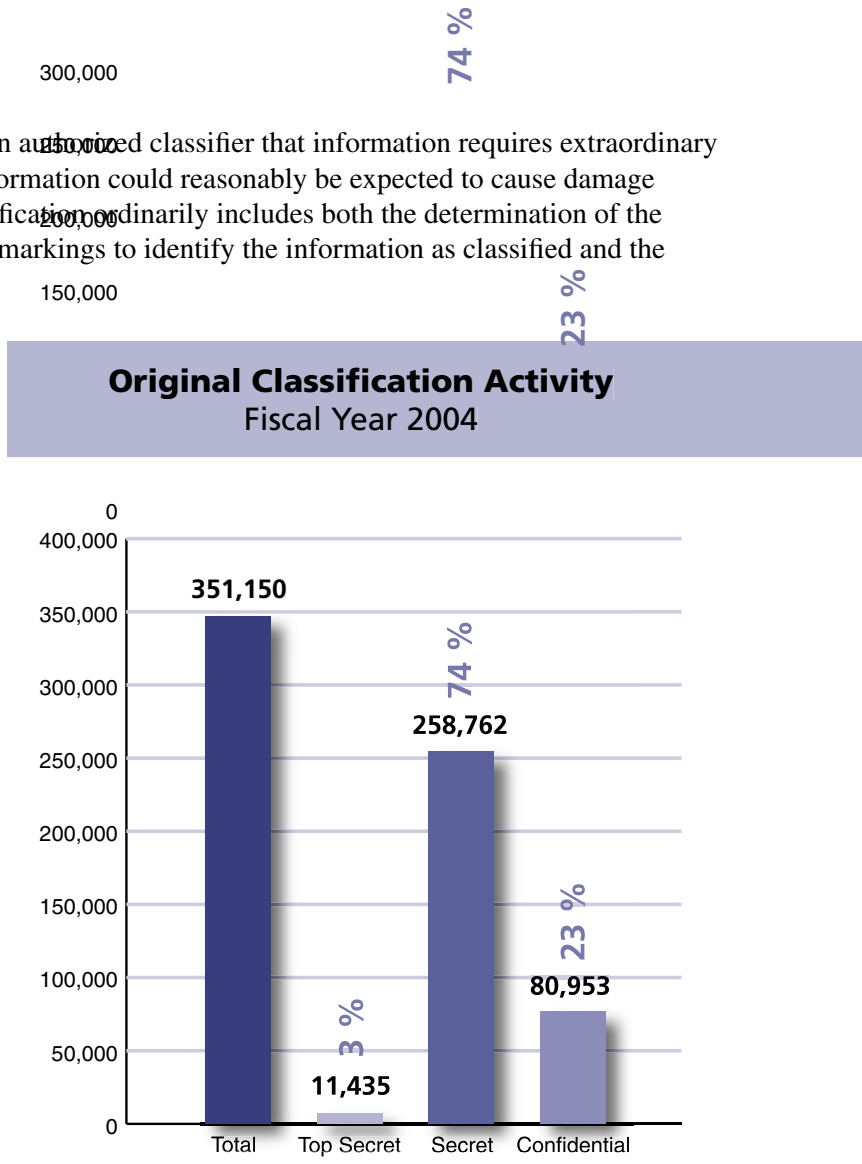
Original Classifiers
Fiscal Year 2004



[1] The Office of the Vice President (OVP) and the Homeland Security Council (HSC) did not report their data to ISOO this year. Therefore, the reported number does not include two OCAs previously reported to ISOO by OVP. Nor do the other data reported here include those for OVP and HSC, which historically have not reported quantitatively significant data.

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 and the date or event when it becomes declassified. By definition, original classification precedes all other aspects of the security classification system, including derivative classification, safeguarding, and declassification. In other words, it is the sole source of newly classified information. The derivative category discussed below is the reutilization of information from the original category. Whereas the derivative category produces many more documents than does original classification, it does not produce new classified information; it merely proliferates that which has already been classified. It is therefore important to remember that original classification is a far more important number on which to focus. Counting the number of derivative documents can be extremely difficult, and in many of the larger agencies the only way to estimate how much is being produced is to collect samples throughout the year and extrapolate a total.

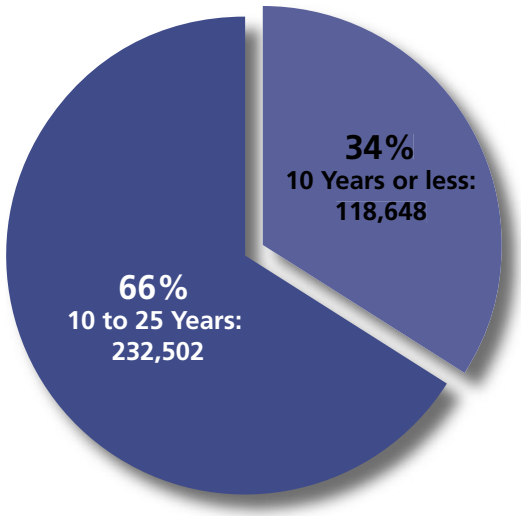


The derivative numbers do not reveal "new secrets in the government," but at best provide a rough indicator of how much work will need to be done by declassification review teams 20 to 25 years from now. At times such as these, a large number of derivative documents can actually be a positive indicator. One of the bitter lessons learned from the terrorist attacks of September 2001 is that counterterrorist information sharing was lacking among the various agencies responsible for protecting the country. Much has been done to correct this deficiency, and increases in the derivative category could reflect increased information sharing. At the same time, each derivative classification decision must be able to trace its origin back to a decision by an original classification authority (thus the primary purpose of the "derived from" line). Derivative decisions that cannot trace their origin or that improperly apply source guidance are a major source of overclassification.

The numbers reported to ISOO for fiscal year 2004 reveal an estimate of 351,150 original classification decisions. This is 113,016 more than what was reported for fiscal year 2003. Most of this increase came from the Department of Defense (DOD), primarily from the Department of the Army (Army). There are several reasons for the increase. In 2004 the ISOO distributed data collection guidance to all activities within the Executive branch, and we have indications that part of this large change in numbers can be attributed to improvements in data collection techniques within the armed forces.[2] Since October 2003 there have been 89 named operations in Iraq and two in Afghanistan. All of these required planning and intelligence preparation that would have to be classified to minimize losses when these operations were launched.

Eighty-nine named operations in the course of only twelve months is a remarkable level of operational activity, but along with this came the requirement to support the operational security needs of units deployed throughout Iraq and Afghanistan. This task alone generated a high volume of classified information. Nevertheless, there were some significant decreases in original classification. These came mainly from the Department of Justice (Justice) (-42 percent) and the Department of State (State) (-3 percent).

During fiscal year 2004, classifiers chose declassification on a specific date or event less than 10 years or on a 10-year date for 118,648 (34 percent) original classification decisions. For the remaining 232,502 (66 percent) original classification decisions, original classifiers elected to apply a declassification date between 10 and 25 years. The 34 percent noted for the 10-year or less category is 18 percentage points lower than what was reported in this category in fiscal year 2003, and it is the lowest reported since fiscal year 1996. Historically, under this Order, agencies selected 10 years or less 52 percent of the time in fiscal year 2003; 57 percent of the time in fiscal year 2002; 54 percent in fiscal year 2001; 59 percent in fiscal year 2000; 50 percent in fiscal year 1999; 36 percent in fiscal year 1998; and 50 percent in fiscal years 1997 and 1996. All original classifiers must remember that automatically defaulting to a 25 year declassification date is not in keeping with the direction of E.O. 12958, as amended. Careful thought must be applied to every classification decision with a view to keeping the information classified no longer than is absolutely necessary. ISOO is very concerned about this substantial increase in classification duration and will place special emphasis on this area during fiscal year 2005.



Duration of Classification
Fiscal Year 2004

[2] In April 2004 ISOO issued detailed data collection guidance to all reporting agencies. See Appendix B.

DERIVATIVE CLASSIFICATION

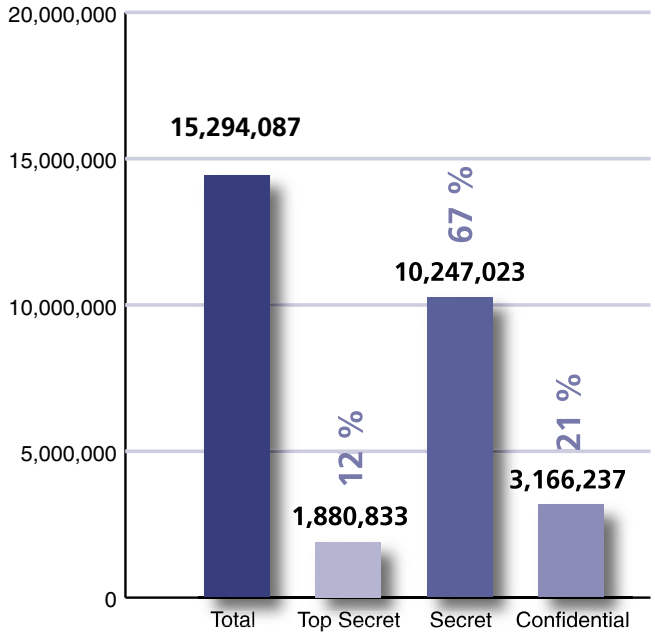
Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form, classified source information. Information may be classified in two ways: (1) through the use of a source document, usually correspondence or publications generated by an OCA; or (2) through the use of a classification guide. A classification guide is a set of instructions issued by an OCA. 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 employees of the Executive branch or a Government contractor with the appropriate security clearance, who are required by their work to restate classified source information, may classify derivatively.

The agencies reported a total of 15,294,087 derivative decisions in fiscal year 2004, which is an increase of 1,300,119, or 9 percent, over what was reported for fiscal year 2003. Here again the largest change came from the DOD, which had an increase of 86 percent. The largest DOD increases came from the activities that are most directly involved in the ongoing operations in Iraq and Afghanistan, namely the Army, the Department of the Navy, which includes the Marine Corps, the U.S. Central Command, the U.S. Pacific Command, and the Defense Intelligence Agency.

In the non-Defense sector there were significant decreases reported by State (-68 percent), the National Reconnaissance Office (NRO) (-39 percent), and DOE (-16 percent). One noteworthy increase came from Justice, whose derivative classification decisions were up 23 percent. This increase has been attributed to an ongoing expansion of counterterrorism analysis at the Federal Bureau of Investigation (FBI). DHS reported an increase of 99 percent, which is a function of the continued development of the Department along with the incorporation of other agencies.

There were several agencies that reported notable changes but yet did not have a great effect on the overall numbers because their volumes were low. These were DOT, the Department of the Interior (Interior), the National Aeronautics and Space Administration (NASA), NSC, the Office of Science and Technology Policy (OSTP), the U.S. Agency for International Development (USAID), and the U.S. Postal Service (USPS).

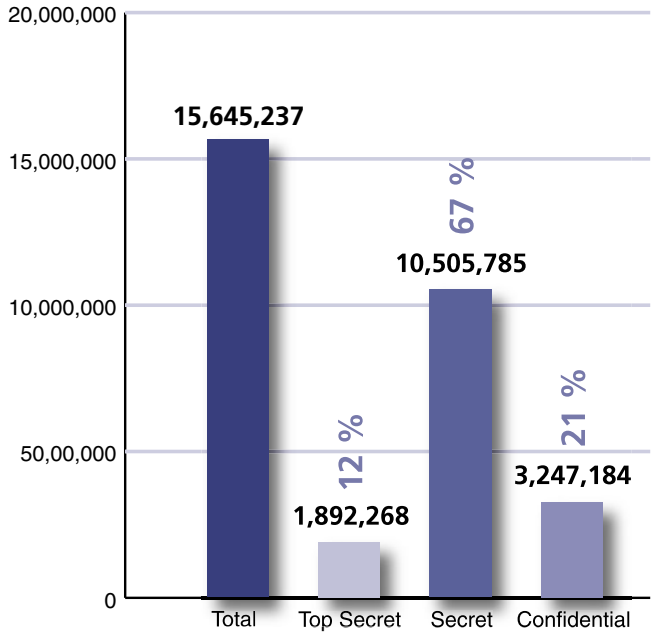
Derivative Classification Activity
Fiscal Year 2004



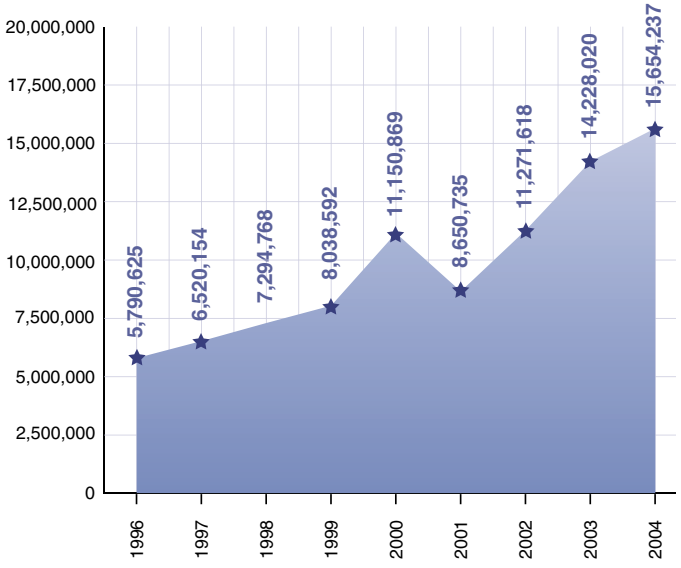
COMBINED CLASSIFICATION

Together, original and derivative classification decisions make up what ISOO calls combined classification activity. In fiscal year 2004, combined classification activity totaled 15,645,237 decisions, which is a 10 percent increase over what was reported for fiscal year 2003. Similar to last year's threat environment, the current geopolitical situation presents unique challenges to our system for classifying and sharing information. While ISOO acknowledges these challenges, it also expects the agencies' commitment to minimizing the information that requires extraordinary protection based solely on the preservation of our national security.

Combined Classification Activity
Fiscal Year 2004



Combined Classification Activity
Fiscal Years 1996 - 2004



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, there was a paradigm shift in our nation's declassification policies. In preceding years, information once classified remained so indefinitely and very often did not become available to the general public, researchers, or historians without persistent and continuous efforts on the part of these individuals. E.O. 12958 changed this paradigm by adding a new "Automatic Declassification" program in addition to the long-standing "Systematic Review for Declassification." Under the "Automatic Declassification" provision of the Order, information appraised as having permanent historical value is automatically declassified at 25 years after classification unless an agency head has determined that it falls within a narrow exemption that permits continued classification, an action that either the President or the ISCAP has approved. 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 provisions until October 14, 2001. It also extended the date of the imposition of the automatic declassification provisions an additional 18 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 deadline would not be met. As a result, work was begun to further amend the Order to extend the deadline. On March 25, 2003, 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 completed the declassification of their eligible records, or to have properly exempted them, referred them to other agencies, or, in the case of special media, appropriately delayed declassification. This amendment also reintroduced the concept of exempting a specific file series from automatic declassification, which originally had been a one-time opportunity.

"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, as amended, 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, for the time being, 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, as amended, reverses the resource burden. Unlike prior systems, in which agencies had to expend resources in order to declassify older information, under the amended order agencies must expend the resources necessary to demonstrate why older historical information needs to remain classified.

Fiscal year 2004 marked the ninth year in which the policies leading up to automatic declassification have been in effect.

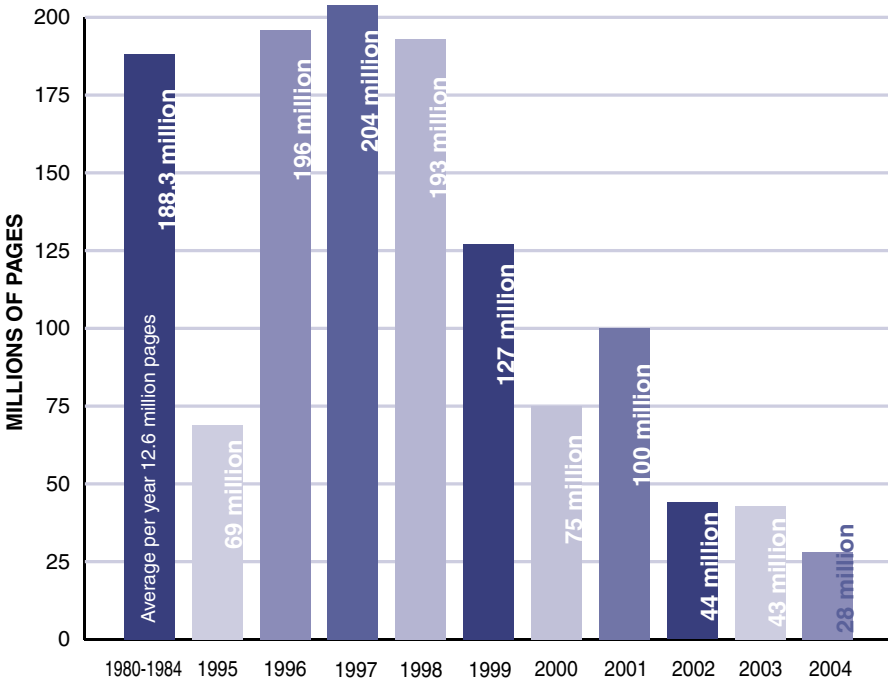
PAGES DECLASSIFIED

During fiscal year 2004, the Executive branch declassified 28,413,690 pages of permanently valuable historical records. This figure represents a 34 percent decrease from that reported for fiscal year 2003. This appears to be a continuance of a downward trend since 1997. Overall, the rate of processing has slowed as a result of several factors, including the increasing complexity of the documents and the number that need to be referred to other equity holding agencies. Naturally, the time to review, identify, and refer such documents is longer than the time to review a document containing solely one's own equity, because of both the concentrated intellectual analysis and the additional administrative processing time. Several agencies have reported problems with funding for contracted support and the loss of key personnel to retirement. Some have changed their methodology from folder level review to document level review, and others are now spending more time reviewing special media. Even so, the number of pages declassified in fiscal year 2004 continues to exceed the yearly average (12.6 million pages) under prior Executive orders.

The number of pages NARA declassified in fiscal year 2004 again declined, from 250,105 pages in fiscal year 2003 to 216,992 pages in fiscal year 2004. In the past three years, NARA's focus has shifted from the actual declassification of other agencies' records to the preparation of records that have been declassified by other agencies for public release. There is also a legislative requirement to perform Quality Assessment Reviews of records that potentially contain sensitive atomic and nuclear weapons information.

Even though its overall output is down by 34 percent, DOD declassified more pages than any other agency in fiscal year 2004, accounting for 71 percent of the total. Six other agencies also reported notable decreases in output: the Central Intelligence Agency, DOE, DOT, Justice, NSC, and USAID.

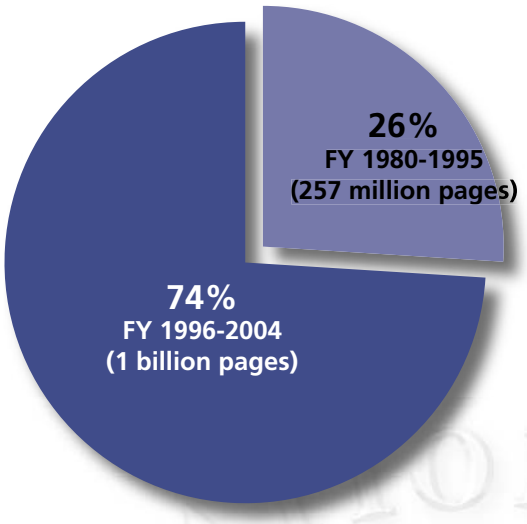
1.27 Billion Pages Declassified
Fiscal Years 1980-2004



Five agencies, NASA, State, DHS, the Overseas Private Investment Corporation (OPIC), and OSTP reported an increase in declassification productivity during fiscal year 2004. ISOO encourages all these agencies to sustain or work to increase their efforts to implement automatic declassification programs to comply with the December 31, 2006, deadline.

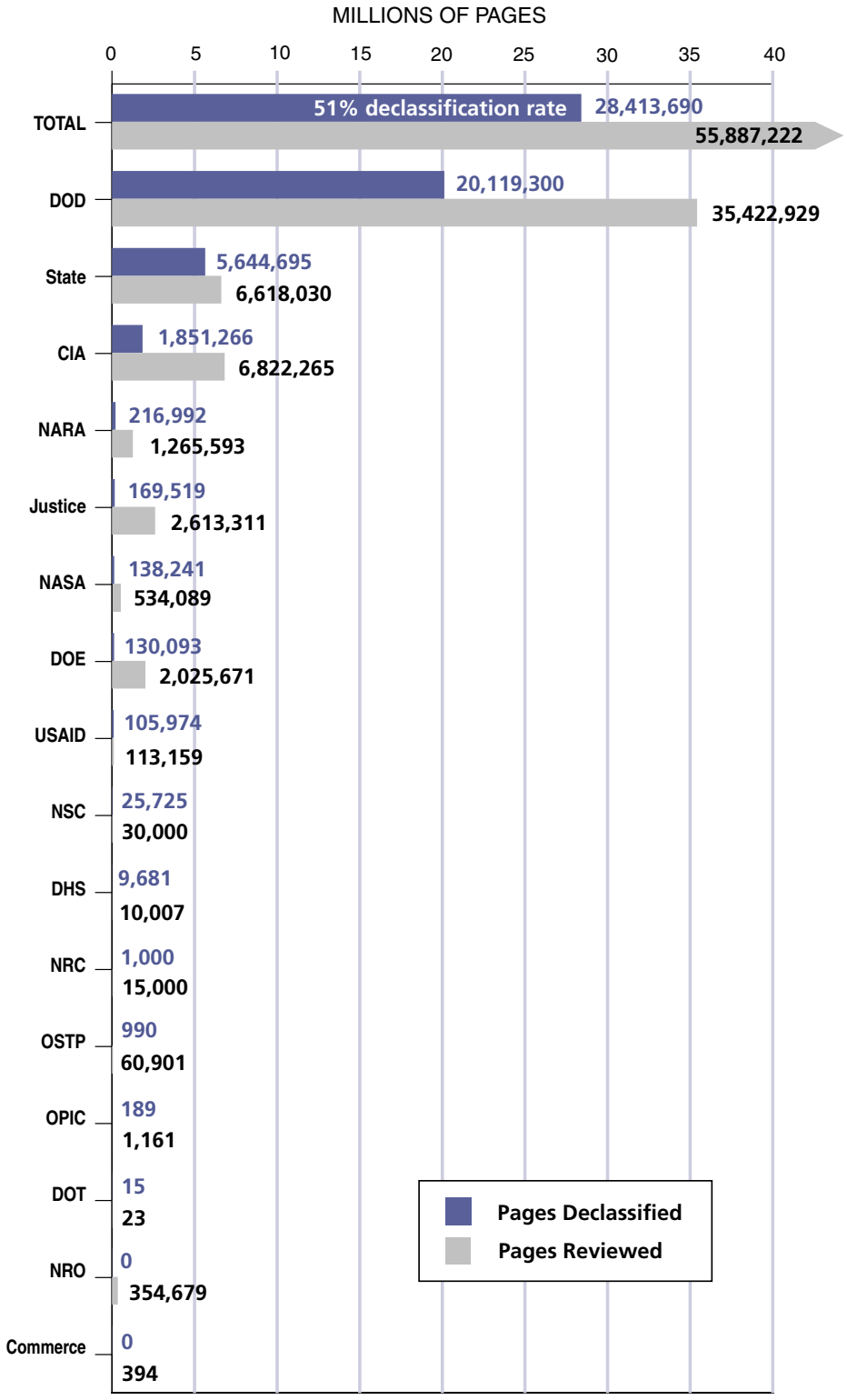
Fiscal year 2004 marks the first time that ISOO has asked the agencies to report on the number of pages reviewed in addition to the number of pages declassified. The intent was that this number would provide a better understanding of the level of effort being applied. The overall numbers reveal we are declassifying 51 percent of the pages being reviewed. However, this percentage varies greatly, with some agencies declassifying a much larger percentage, and others significantly less.

In the nine years that Executive Order 12958 has been in effect, Executive branch agencies have declassified more than 1 billion pages of permanently valuable historical records. Compared with 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 nine 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 fiscal year 1980, it has reported the declassification of permanently valuable records totaling approximately 1.27 billion pages. Of that total, 1.028 billion pages, or 81 percent, have been declassified, in large part because of the automatic declassification provisions of E.O. 12958 and its amendments.

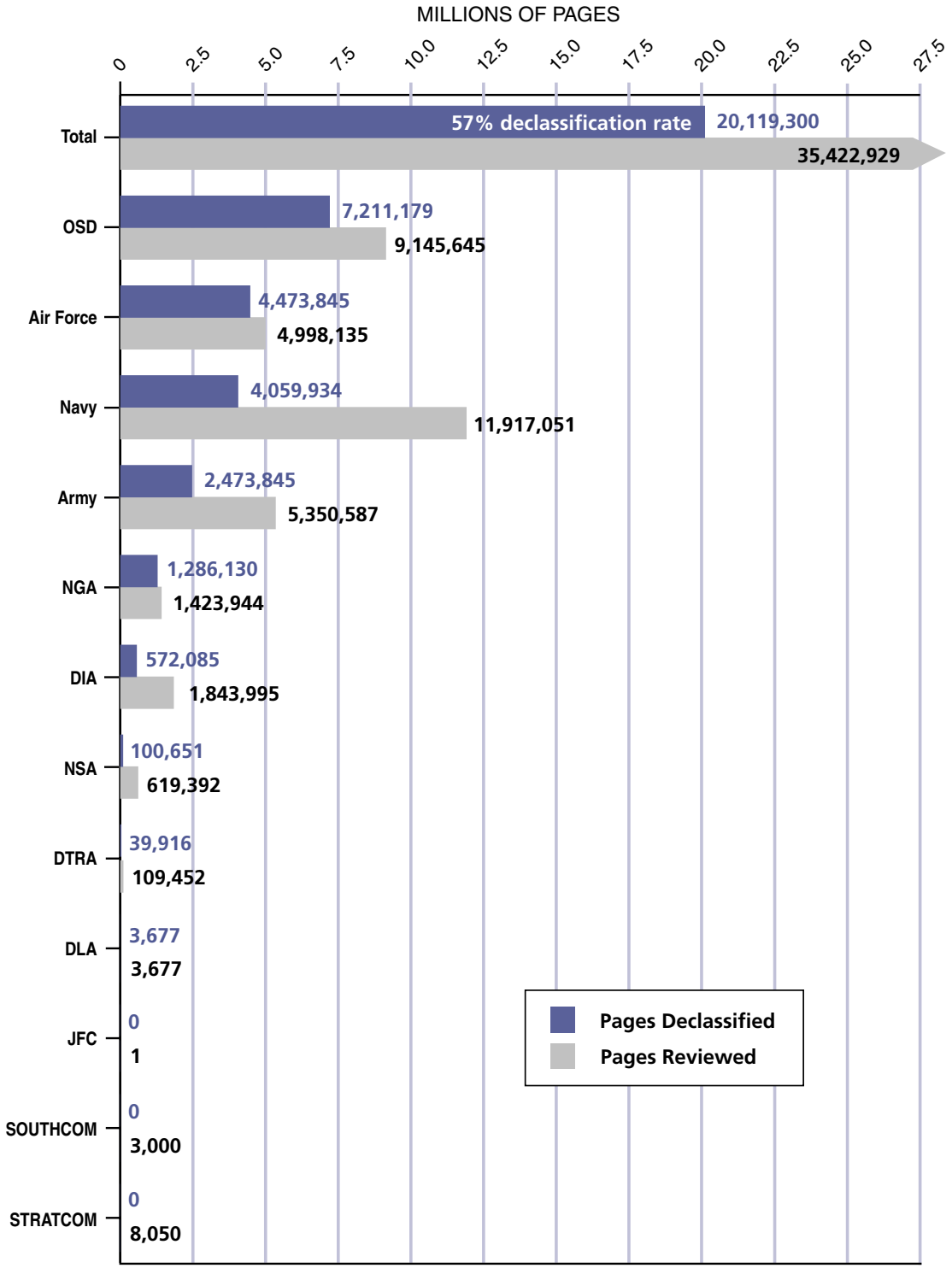


1.27 Billion Pages Declassified
Fiscal Years 1980-2004

Number of Pages Declassified by Agency
Fiscal Year 2004



DOD Components: Pages Declassified by Activity Fiscal Year 2004



PROGRESS TOWARD THE AUTOMATIC DECLASSIFICATION DEADLINE OF DECEMBER 31, 2006

In order to assess Executive branch progress toward fulfilling the commitment to the December 31, 2006, deadline, we requested that all agencies provide information about their declassification programs to ISOO for review and evaluation. The request was sent to those agencies that are original classifiers and/or derivative classifiers, as well as to those that are solely consumers or holders of classified national security information.

Based on this year's initial data, as of December 31, 2003, we estimate there were 260 million pages of classified national security information that must be declassified, exempted, or referred to other agencies by December 31, 2006. This figure is in addition to the 982 million pages declassified in the prior eight years that automatic declassification has been in effect. We believe, for the most part, that the Executive branch is progressing toward fulfilling its responsibilities for these records by the deadline, although a significant number of agencies remain at risk of not meeting it.

Forty-six agencies possessing records subject to Section 3.3 of the Order were asked to submit declassification plans. As of August 2004, we are confident that 25 of those agencies will be prepared for the implementation of the automatic declassification program by the deadline. Collectively, these 25 agencies account for 45 percent of the total number of pages subject to automatic declassification. ISOO needs to work closely with the remaining 21 agencies to ensure that they allocate sufficient resources to meet the requirement.

Those agencies that are on or ahead of schedule with respect to their estimated pages requiring review have several common characteristics, including excellent management support, an adequate budget, stable staffing, and a sound review process.

ISOO noted a number of highly effective business practices with respect to the implementation of the automatic declassification program that warrant special mention. Several agencies have established an organizational structure that ensures close coordination between their declassification, the Freedom of Information Act, and records management programs. This is a noteworthy best practice that ensures both increased efficiency and consistency. We are especially pleased with a number of agencies that are playing leading roles in initiatives such as the Interagency Referral Center housed in NARA.

Another noteworthy organizational approach that has proven successful is a centralized declassification coordinator who oversees all declassification reviews and referrals regardless of where they may occur within the agency. This facilitates any referrals from external agencies and helps ensure that such referrals are directed to the appropriate office of program responsibility (OPR).

Yet another characteristic of the more successful agencies is a solid working relationship among agency offices of security, declassification, and records management. Such cooperation is evidenced in integrated teams that coordinate, communicate, and resolve issues dealing with classification, declassification, and records management. Declassification oversight committees are especially beneficial in refereeing and resolving conflicts regarding difficult release decisions.

Agencies that have less successful programs and that risk not meeting the deadline have inadequate management support, underfunded budgets, fewer well trained staff, high turnover rate, and little to no process for reviewing or coordinating records. A secondary factor for several agencies is that they are only now starting the process of identifying records for review.

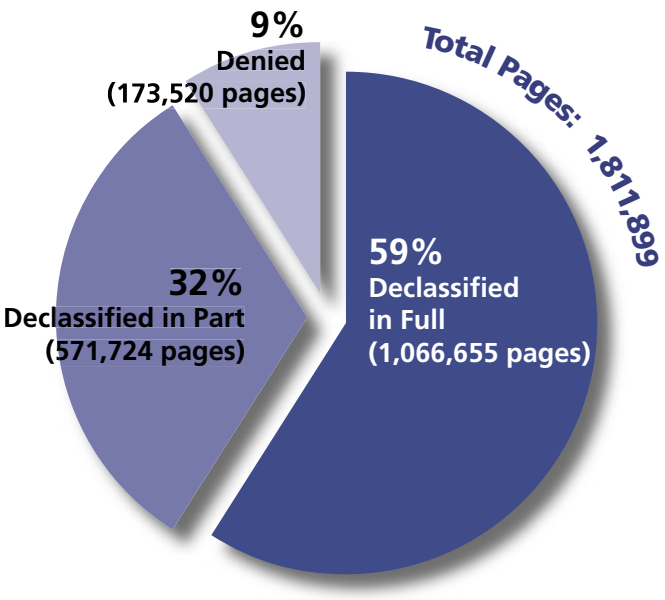
We will continue to work with all agencies and offer what assistance we can to keep the process moving forward. We have emphasized to each agency head that automatic declassification is an ongoing program that begins, not ends, on December 31, 2006.

MANDATORY DECLASSIFICATION REVIEW

Under Executive Order 12958, as amended, the MDR process permits individuals or agencies to require the review of specific national security information for the purpose of seeking its declassification. Requests must be in writing and must describe the information with sufficient detail to permit retrieval with a reasonable amount of effort. MDR remains popular with some researchers as a less contentious alternative to requests under the Freedom of Information Act, as amended (FOIA). It is also used to seek the declassification of presidential papers or records not subject to the FOIA.

INITIAL REQUESTS

Agencies processed 4,470 initial requests for MDR during fiscal year 2004. Although this represents a decrease of 786 from fiscal year 2003, it is greater than the 3,874 average number of initial requests for MDR processed annually for fiscal year 1996 through fiscal year 2003. The total number of pages processed during fiscal year 2004 was 304,375. This represents a decrease of 5,798 as compared to fiscal year 2003. However, the number of pages processed in fiscal year 2004 was significantly larger than the 188,440 average number of pages processed annually for fiscal year 1996 through fiscal year 2003.



Disposition of Initial MDR Requests
Fiscal Years 1996-2004

The processing of initial requests for MDR during fiscal year 2004 resulted in the declassification of information in 288,785 pages, or 95 percent of the pages processed. Specifically, it resulted in the declassification of 224,342 pages in full (74 percent) and 64,443 pages in part (21 percent). Only five percent, or 15,590 pages, remained classified in their entirety after being reviewed. As demonstrated to the left, MDR remains a very successful means of declassifying information, resulting in information being declassified in 91 percent of the pages processed during fiscal years 1996-2004.

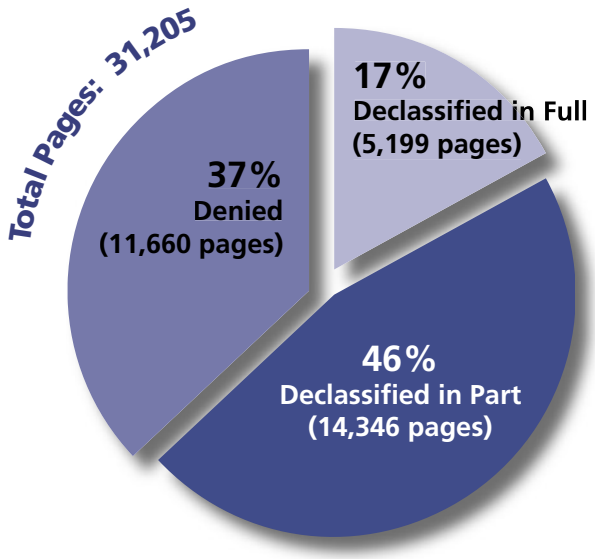
APPEALS

During fiscal year 2004, agencies processed 163 appeals of agency decisions to deny information during the processing of initial requests for MDR. This represents a significant increase from fiscal year 2003, when agencies processed only 58 MDR appeals. Fiscal year 2004 represents the second largest number of MDR appeals processed in a single fiscal year since the issuance of E.O. 12958 and is well above the average of 93 appeals processed annually for fiscal year 1996 through fiscal year 2003. Agencies processed 6,134 pages as part of these MDR appeals, representing a significant increase over the 2,339 pages processed in fiscal year 2003 and the average of 3,133 pages processed annually for fiscal year 1996 through fiscal year 2003. In fact, fiscal year 2004 represented the largest number of pages processed as part of MDR appeals since the fiscal year 1996 issuance of E.O. 12958.

The processing of MDR appeals by agencies during fiscal year 2004 resulted in the declassification of information in 3,889 pages, or 63 percent of the pages processed. Specifically, it resulted in the declassification of 296 pages in full (5 percent) and 3,593 pages in part (58 percent). Only 37 percent, or 2,245 pages, remained classified in their entirety after being reviewed.

As the chart to the right demonstrates, information is often declassified on appeal, suggesting that requesters can anticipate greater returns in declassified information if they pursue an appeal.

Any final decision made by an agency to deny information during a MDR appeal may be appealed by the requester directly to the ISCAP, and the agency is required by E.O. 12958, as amended, to notify the requester of these appeal rights. Should an agency fail to meet the timeframes indicated in Article VIII, section A(3) of Appendix A to 32 C.F.R. Part 2001, agencies, requesters, and appellants should be aware that initial requests for MDR, and MDR appeals, may be appealed directly to the ISCAP.



Disposition of MDR Appeals
Fiscal Years 1996-2004

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

Telephone: **202.219.5250**
Fax: **202.219.5385**
Email: **iscap@nara.gov**

Additional information about MDR can be found in: (1) sections 3.5 and 3.6 of E.O. 12958, as amended; (2) 32 C.F.R. Part 2001.33; and (3) Article VIII of Appendix A to 32 C.F.R. Part 2001. Please also consult the following portion of the ISOO website:

http://www.archives.gov/isoo/oversight_groups/iscap/mdr_appeals.html

PUBLIC INTEREST DECLASSIFICATION BOARD

INTRODUCTION

In establishing the Public Interest Declassification Board, the President and Congress determined that it is in the national interest to establish an effective, coordinated, and cost-effective means by which records on specific subjects of extraordinary public interest that do not undermine the national security interests of the United States may be collected, retained, reviewed, and disseminated to policymakers in the executive branch, Congress, and the public.

PURPOSE

- The Board advises the President and other executive branch officials on the systematic, thorough, coordinated, and comprehensive identification, collection, review for declassification, and release of declassified records and materials that are of archival value, including records and materials of extraordinary public interest.
- The Board promotes the fullest possible public access to a thorough, accurate, and reliable documentary record of significant U.S. national security decisions and significant U.S. national security activities in order to:
  - support the oversight and legislative functions of Congress;
  - support the policymaking role of the executive branch;
  - respond to the interest of the public in national security matters; and
  - promote reliable historical analysis and new avenues of historical study in national security matters.
- The Board provides recommendations to the President for the identification, collection, and review for declassification of information of extraordinary public interest that does not undermine the national security of the United States.
- The Board advises the President and other executive branch officials on policies deriving from the issuance by the President of Executive orders regarding the classification and declassification of national security information.
- The Board reviews and makes recommendations to the President with respect to any congressional request, made by the committee of jurisdiction, to declassify certain records or to reconsider a declination to declassify specific records.[3]

MEMBERSHIP

The Board is composed of nine individuals appointed from among citizens of the United States who are preeminent in the fields of history, national security, foreign policy, intelligence policy, social science, law, or archives. Current members are:

L. Britt Snider, Chair

Martin Faga	Steven Garfinkel
Joan Vail Grimson	Elizabeth Rindskopf Parker
David Skaggs	Richard Norton Smith

The Director of the Information Security Oversight Office serves as Executive Secretary to the Board.

---

[3] Responsibility added by Section 1102 of the Intelligence Reform and Terrorism Prevention Act of 2004, which also extended the life of the Board.

ISOO INSPECTIONS

SUMMARY OF ACTIVITY

In fiscal year 2004, ISOO expanded the breadth of its inspection program under E.O. 12958, reviewing 23 agencies, which included a mix of military and civilian agencies of varying sizes. Overall, these agencies were satisfactorily implementing the requirements of the Order pertinent to their activity. ISOO found a number of agencies with very strong programs to protect classified national security information as well as some that need improvement, particularly in the areas of security education and training, and self-inspections. For example, we found 19 education and training programs that either lacked refresher training or had refresher training that did not cover all required topics. More specifically, it was evident that agency security managers need to focus refresher training on the proper application of classification markings.

ISOO found that many agencies need to either establish or improve their self-inspection program, and that the inclusion of a document review was a necessary improvement. We also determined that 15 percent of the agencies had inadequate staffing levels to meet their internal oversight responsibility. Additionally, the findings show that many agencies have yet to update their internal security regulations despite the fact that the amendment to the Order became effective more than one year ago. Many agencies need to improve their procedures for conducting an inquiry/investigation of a loss, possible compromise, or unauthorized disclosure to include reporting compromises of classified information to the Director of ISOO. In analyzing such security violations, downloading documents from classified information systems, such as SIPRNET or CLASSNET, without ensuring proper classification markings was a recurring problem for many of the agencies inspected.

ISOO DOCUMENT REVIEWS

Another important element of ISOO inspections is a validation of the agency's classified product. During our visits we reviewed a total of 2,021 documents, of which 1,022 contained discrepancies, yielding an error rate of 51 percent.

Declassification and portion marking were the biggest problem areas. Some agencies are inconsistent in the application of portion markings. This is especially true regarding graphic presentations, a category of document that is frequently ignored when it comes to marking portions. Additionally, the basis for classification could not be determined for 10 percent of the documents, making the appropriateness of the classification suspect. Five percent of the documents had the indefinite instruction for the duration of classification, "Originating Agency's Determination Required" (OADR), which has not been a valid marking since 1995.[4] As noted earlier, these omissions contribute to the specter of overclassification within agencies.

[4] Section 1.4 of E.O. 12958, as amended, requires that the "Declassify on" line should contain one of the following: (1) date or event less than 10 years; (2) a date 10 years from the date the information/document was created; (3) a date greater than 10 years and less than 25 years from the date of the information/document; and (4) a date 25 years from the date of the decision. "OADR" may not be cited when the source document is dated later than October 13, 1995, the effective date of Executive Order 12958. Also, the X1 through X8 exemption codes may not be cited when the source document is dated later than September 22, 2003, the effective date of ISOO Directive No. 1, the implementing directive for Executive Order 12958, as amended.

BEST PRACTICES

Some agencies were innovative in making their security awareness training products both informative and attention grabbing. For example, both the General Services Administration's central security office and the Defense Intelligence Agency have developed security education and training programs based on popular themes.

CONCLUSION

The variation in performance among the agencies correlates very closely to the level of support that senior management gives the program at each agency. ISOO will focus on the marking discrepancies through our upcoming inspections. In particular, we will ensure that agencies are conducting quality internal document reviews to ensure that the classified product is meeting the requirements of the Order. Additionally, we will ensure that agencies improve their security education and training, especially the emphasis in classification markings, in refresher training. ISOO inspections will continue to monitor agency implementation of the requirements of the Order and strive to help improve agencies' performance.

APPENDIX A:

Declaration of Principles for Reciprocity of Access Eligibility Determinations Within Industry

Delays in security clearances and in access to highly sensitive programs (Sensitive Compartment Information, Special Access Programs, Q Clearances, and similar programs) are a matter of concern from an economic, technological, and national security perspective. Failure to reciprocally honor clearance and access actions by another agency hampers industry's ability to be responsive to Government's needs. In addition, as agencies struggle to reduce processing times, mutual and reciprocal acceptance of investigations and adjudications by all agencies makes even more sense today. Duplicative actions create unnecessary delays, needlessly consume limited resources, and place national security at risk by further delaying the return of equilibrium to the personnel security clearance process.

In furtherance of Executive Order 12968, "Access to Classified Information," Section 2.4, reciprocal acceptance of access eligibility determinations by National Industrial Security Program (NISP) cognizant security authorities (CSAs) for industrial personnel will be implemented in the following manner:

Collateral Security Clearances

- An employee with an existing security clearance (not including an interim clearance) who transfers or changes employment status (e.g., contractor to contractor or government to contractor, etc.) is eligible for a security clearance at the same or lower level at the gaining activity without additional or duplicative adjudication, investigation, or reinvestigation, and without any requirement to complete or update a security questionnaire unless the gaining activity has substantial information indicating that the standards of Executive Order 12968 may not be satisfied.
    - The "substantial information" exception to reciprocity of security clearances does not authorize requesting a new security questionnaire, reviewing existing background investigations or security questionnaires, or initiating new investigative checks (such as a credit check) to determine whether such "substantial information" exists
    - The gaining activity may request copies of background investigations and/or security questionnaires from the existing or losing activity for purposes of establishing a personnel security file, but eligibility for a reciprocal security clearance may not be delayed nor may there be additional or duplicative adjudication after the documents are received.
    - A security clearance is confirmed by the CSA of the gaining activity by verifying with the existing or losing activity or its CSA, as appropriate, the level of and basis for the security clearance. Where possible, automated data bases should be used to confirm security clearances.
- If the most recent investigation is not "current" in accordance with approved investigative standards an employee will immediately be granted a security clearance at the gaining activity provided the employee has completed and submitted all appropriate questionnaires, waivers, and fingerprints at either the losing or gaining activity.

Highly Sensitive Programs

- "Highly sensitive programs" means Sensitive Compartmented Information, Special Access Programs, Q Clearances, and other similar programs.
- The principles of reciprocity for collateral security clearances set forth above are also applicable for access to highly sensitive programs with the following exceptions:
    - Where the sensitivity level of the new highly sensitive program is not the same as the existing program to which the employee has access; or
    - Where the existing access to a highly sensitive program is based, under proper authority, on a waiver of or deviation from that program's adjudicative or investigative guidelines, or where the access is conditional, interim, or temporary.
- The sensitivity level of highly sensitive programs is determined from the investigative and adjudicative standards that are established at the time the program is approved; if programs use the same criteria for determining access, they are at the same sensitivity level.
- If additional adjudication or investigation is necessary because a highly sensitive program is not at the same sensitivity level as the program to which the employee currently has access, only additional - not duplicative - investigative or adjudicative procedures may be pursued. Any additional investigative or adjudicative procedures will be completed in a timely manner.

Reporting of Practices Inconsistent with These Principles

- Each CSA shall designate in writing a point of contact for industry to report practices contrary to these principles, and the points of contact will be published on appropriate websites, such as sites of the Defense Security Service, the Information Security Oversight Office, and CSAs.
- Any such reports shall be submitted through the corporate security office for each cleared company/ corporation and will be resolved in a timely manner. In cases where only one sector or division of a corporation is cleared, the corporation shall establish a cleared contact in that sector or division to accept reports for the corporation.
- For the purpose of establishing statistics regarding the effectiveness of this declaration, CSA points of contact and industry shall provide copies of reports of practices contrary to these principles and their resolution to the Information Security Oversight Office.

APPENDIX B:
Guidelines for SF 311 Data Collection

What to Count

The SF 311 asks for the number of "classification decisions contained in finished products for dissemination or retention, regardless of the media. Do not count reproductions or copies." "Regardless of the media" includes finished products that are not necessarily on paper, such as, but not limited to, the following:

- official correspondence circulated by e-mail
- reports and/or intelligence products circulated or posted electronically
- books
- maps
- photographs
- presentations including slides and transparencies
- inputs and outputs from database records that are considered to be finished products

The Information Security Oversight Office realizes that most classified e-mail messages are not finished products. For example, routine analyst-to-analyst exchanges of information and analytic interpretation on a classified topic would not be considered a finished product. However, if these same exchanges are required by law and regulation to be retained for record purposes, that would be considered a finished product.

What Not to Count

Again, do not count anything that you do not consider to be a "finished product for dissemination or retention." This means that most of your e-mail messages probably do not need to be counted. If you have an e-mail message that fits the definition of "finished product for dissemination or retention," you count it as one document without counting how many addresses it went to, or how many times it appears in e-mail threads. This is consistent with the directions on the SF 311 form, where it says "Do not count reproductions or copies." If there is a classified e-mail with classified attachments, generally both would be counted. If the e-mail is merely a transmittal vehicle for a classified attachment and contains no classified information itself, the e-mail would not be counted, but the attachment would. This presumes that the sender is also the originator/author of the classified attachment.

Counting Original Classification Decisions

When possible, use an actual count for determining the number of original decisions. If an actual count is not possible, then the same sampling guidelines discussed below may also be used to estimate original classification decisions.

Counting Derivative Classification Decisions

For many large agencies and organizations it is not possible to conduct actual counts of derivative classification decisions. In such cases a sampling method should be used.

Steps for Sampling

1. Define the Total Population

The first step in this process is to determine which level of your organization should be sampled. For example, for some organizations it might be best to sample from the total population of department heads; for another it might be the total population of original classification authorities (OCAs). Please indicate which level of the organization is sampled in Part I of the SF 311.

2. Collect Samples

The most common practice for collecting samples is to ask each respondent to provide numbers for a two-week period during each quarter of the fiscal year. Respondents should include all types of media (e.g., word processing documents, presentations, or e-mails) – see "What to Count" above. Again, when counting e-mail, if there is both a classified e-mail and any classified attachments, both could be counted. If the e-mail is merely a transmittal vehicle for a classified attachment and contains no classified information itself, the e-mail should not be counted, but the attachment should. A sample tally sheet to collect data is provided with this enclosure. Action officers/ respondents may wish to use this sheet as a means of recording data about classification actions they make in a particular sampling period.

The samples will provide data for a total of eight weeks of activity distributed across the fiscal year. Various multipliers can then be applied to the data to reach an estimate for the entire 52-week year. One way to do this would be to apply a multiplier of 6.5 to each response to achieve a 52-week total for each respondent. Another way would be to average out all the two-week responses into one typical two-week period for the entire organization and then multiply this by 26 to reach the 52-week total. Please explain the methodology you employ in Part I of the SF 311. (See example on next page.)

Example

Method 1

Command A has four organizations, and the security manager has tasked each one to request that their action officers track the number of derivative classification decisions each makes during a two-week period in November, two weeks in February, two weeks in May, and two weeks in August. Once the security manager obtains a total sample by adding the results of the four quarterly samples, each Sample Total is then multiplied by 6.5, which yields a Total Estimate for the fiscal year. These figures can then be entered in Blocks 19, 20, 21, and 22 on the SF 311.

November	February	May	August	Sample Totals	Multiplie	Total Estimate	on SF 311
TS 1	TS 5	TS 0	TS 21	TS 27	X 6.5=	175.5	Block 19
S 70	S 250	S 60	S 80	S 460	X 6.5 =	2990	Block 20
C 25	C 25	C 100	C 40	C 190	X 6.5 =	1235	Block 21
						4400.5	Block 22
						Total Derivative	

Method 2

Another way to perform the calculations is to average out the four two-week samples and apply a multiplier of 26 instead of 6.5.

November	February	May	August	Sample Totals	Multiplie	Total Estimate	on SF 311
TS 1	TS 5	TS 0	TS 21	TS 6.75	X 26 =	175.5	Block 19
S 70	S 250	S 60	S 80	S 115	X 26 =	2990	Block 20
C 25	C 25	C 100	C 40	C 47.5	X 26 =	1235	Block 21
						4400.5	Block 22
						Total Derivative	

Agency Acronyms or Abbreviations

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
DCMA:	Defense Contract Management Agency
DeCA:	Defense Commissary Agency
DFAS:	Defense Finance and Accounting Service
DHS:	Department of Homeland Security
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
Ex-Im Bank:	Export-Import Bank of the United States
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
HSC:	Homeland Security Council
HUD:	Department of Housing and Urban Development
Interior:	Department of the Interior
ISCAP:	Interagency Security Classification Appeals Panel
ISOO:	Information Security Oversight Office
JCS:	Joint Chiefs of Staff
Justice:	Department of Justice
Labor:	Department of Labor
MCC:	Millennium Challenge Corporation
MDA:	Missile Defense Agency
MMC:	Marine Mammal Commission
MSPB:	Merit Systems Protection Board
NARA:	National Archives and Records Administration
NASA:	National Aeronautics and Space Administration
Navy:	Department of the Navy
NGA	National Geospatial-Intelligence Agency
NISP:	National Industrial Security Program
NISPPAC:	National Industrial Security Program Policy Advisory Committee
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
PIDB:	Public Interest Declassification 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
USAID:	United States Agency for International Development
USCENTCOM:	United States Central Command
USDA:	United States Department of Agriculture
USITC:	United States International Trade Commission
USMC:	United States Marine Corps
USPACOM:	United States Pacific Command
USPS:	United States Postal Service
USTR:	Office of the United States Trade Representative
VA:	Department of Veterans Affairs

INFORMATION SECURITY OVERSIGHT OFFICE

National Archives Building
700 Pennsylvania Avenue, N.W., Room 500
Washington, D.C. 20408-0001

(202) 219-5250 phone
(202) 219-5385 fax

Email: isoo@nara.gov
Website: www.archives.gov/isoo