

A large, stylized American flag is positioned on the left side of the page, partially overlapping the text. The stars are white on a dark blue field, and the stripes are white and dark blue.

# 2007

## REPORT TO THE PRESIDENT

---

Information Security Oversight Office



## 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).

## MISSION

---

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

## FUNCTIONS

---

- Develops implementing directives and instructions.
- Maintains liaison with agency counterparts and conducts on-site reviews 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 Executive orders.
- Reviews and approves agency implementing regulations and agency guides for systematic declassification review.

## GOALS

---

- Promotes and enhances the system that protects the national security information that safeguards the American Government and its people.
- Provides 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.
- Promotes and enhances concepts that facilitate the sharing of information in the fulfillment of mission-critical functions related to national security.
- Provides expert advice and guidance pertinent to the principles of information security.



# LETTER TO THE PRESIDENT

---

May 30, 2008

The President  
The White House  
Washington, DC 20500

Dear Mr. President:

I am pleased to submit the Information Security Oversight Office's (ISOO) Report to the President for Fiscal Year 2007.

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 provides statistics and analysis concerning key components of the system, primarily classification and declassification, and coverage of ISOO's on-site reviews. 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."

More than five years have passed since your March 2003 amendment of the policy that serves as the foundation of the classification system and much of the policy has been in effect for more than twelve years. The program is, on balance, working well. However, despite the stability in the policy, our on-site reviews continue to find shortcomings in agency implementation of core elements of the program.

In order to remain effective, the security classification system requires constant attention. In addition to the ISOO staff, thousands of individuals in Government and industry are responsible for administering the security classification system and diligently work to enhance its performance. Yet, the classification, safeguarding, and declassification of classified national security information all require an increased effort by agencies. We will enhance our oversight with additional measures to communicate general areas of concern identified through our on-site reviews to all agencies with responsibility for classified national security information.

Respectfully,



William J. Bosanko  
Director



# TABLE OF CONTENTS

---

Summary of FY 2007 Program Activity .....	1
Classification.....	2
Declassification .....	8
Interagency Security Classification Appeals Panel.....	19
On-Site Reviews .....	23
National Industrial Security Program .....	26
Report on Cost Estimates for Security Classification Activities .....	27
Agency Acronyms and Abbreviations .....	30



# SUMMARY OF FISCAL YEAR 2007 PROGRAM ACTIVITY

---

## Classification

- Executive branch agencies reported 4,128 original classification authorities.
- Agencies reported 233,639 original classification decisions.
- Executive branch agencies reported 22,868,618 derivative classification decisions.
- Agencies reported 23,102,257 combined classification decisions.

## Declassification

- Under Automatic and Systematic Review Declassification programs, agencies declassified 37,249,390 pages of historically valuable records.
- Agencies received 7,827 new mandatory declassification review requests.
- Under mandatory declassification review, agencies declassified 347,338 pages in their entirety; declassified in part 84,033 pages; and retained classification of 30,125 pages in their entirety.
- Agencies processed 104 mandatory declassification review appeals.
- On appeal, agencies declassified in their entirety or in part 5,346 additional pages.





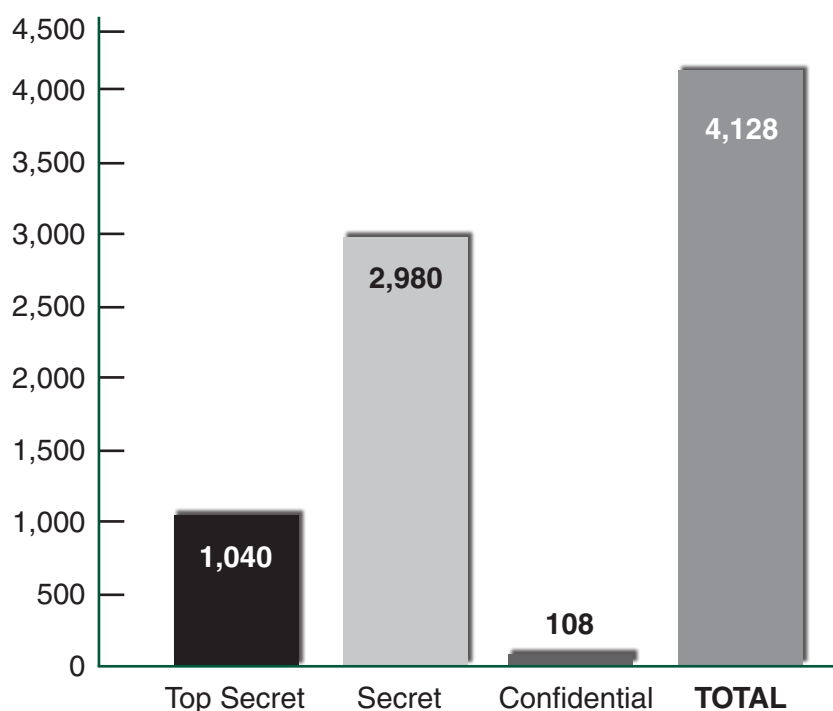
# CLASSIFICATION

## Original Classifiers

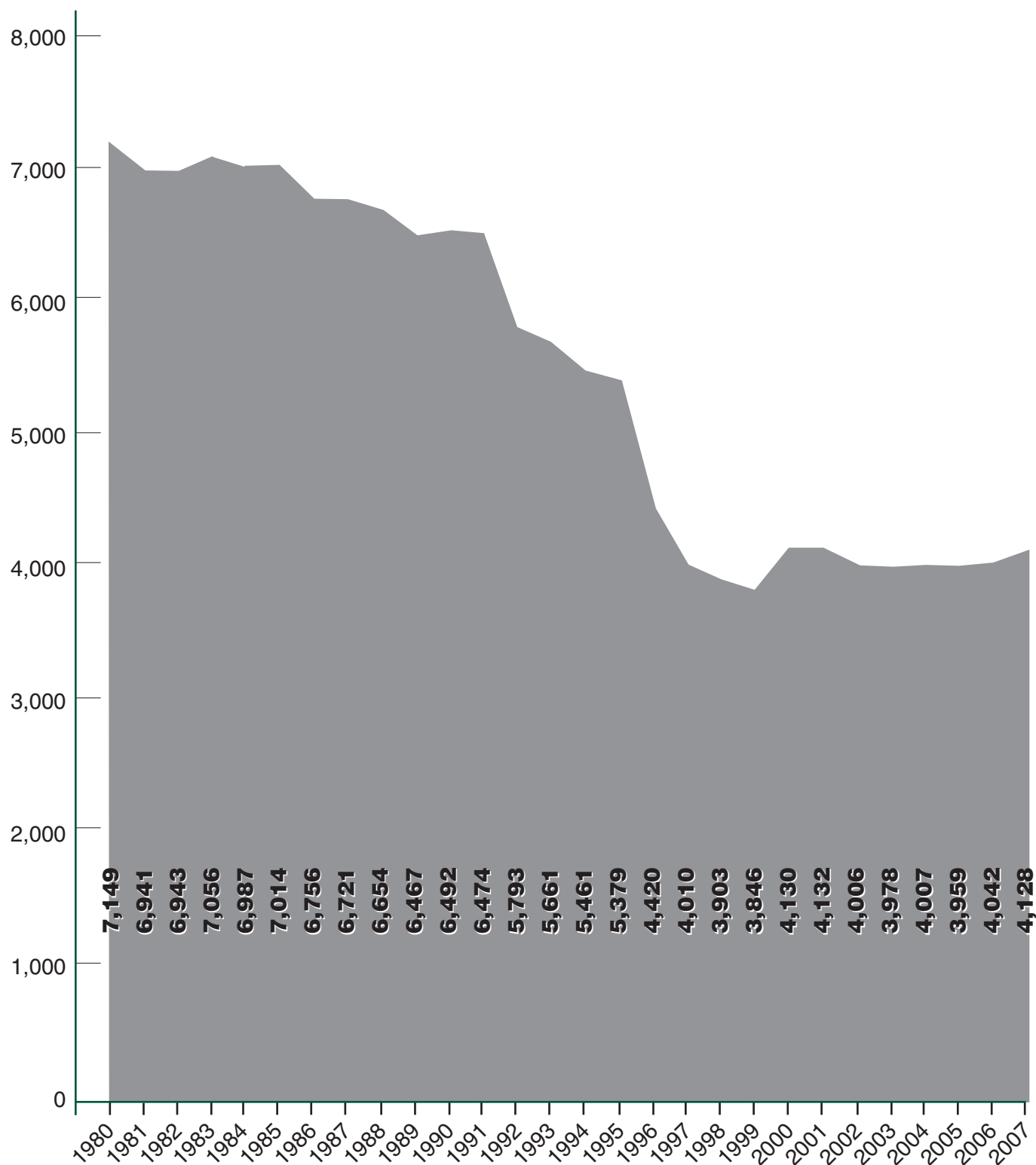
**O**riginal classification authorities (OCAs), also called original classifiers, are those individuals designated in writing, either by the President, by selected agency heads, or by designated senior agency officials with Top Secret original classification authority, to classify information in the first instance. Under E.O. 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 be able to identify or describe the damage. During FY 2007, the number of OCAs increased from 4,042 to 4,128, which represents an increase of two percent. In 1980 ISOO first reported on the number of OCAs, which at that time numbered 7,149. The average number of OCAs from FY 1980 to FY 2006 is 5,352.

### Original Classification Authorities, FY 2007



## Total Number of Original Classification Authorities Since 1980

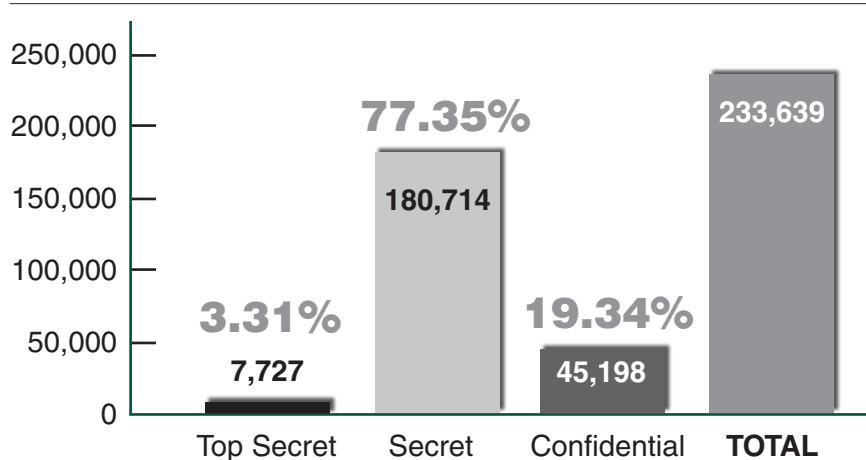


## Original Classification

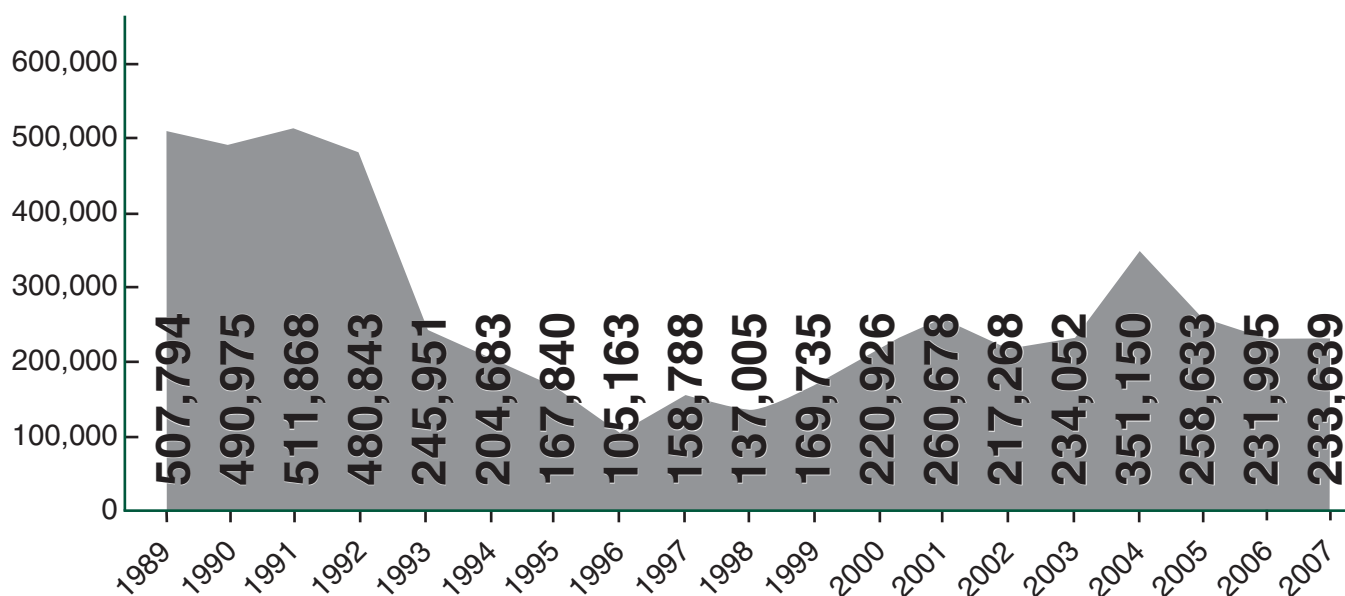
**O**riginal classification is an initial determination by an OCA that information owned by, produced by or for, or is under the control of the United States Government, requires protection because unauthorized disclosure of that information could reasonably be expected to cause damage to national security. Additionally, the process of original classification must

always include a determination by an OCA of the concise reason for the classification that falls within one or more of the authorized categories of classification, the placement of markings to identify the information as classified, and the date or event when the information becomes declassified. By definition, original classification precedes all other aspects of the security classification system, including derivative classification, safeguarding, and declassification.

### Original Classification Activity, FY 2007



### Original Classification Activity, FY 1989 - FY 2007

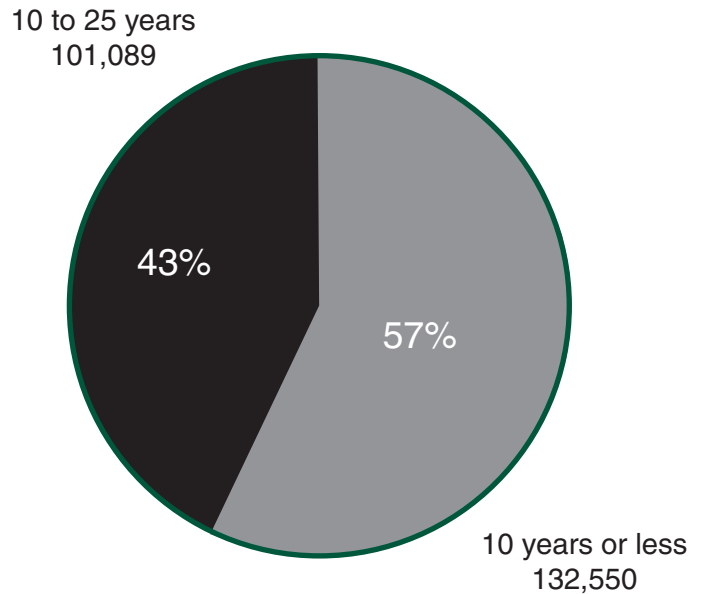




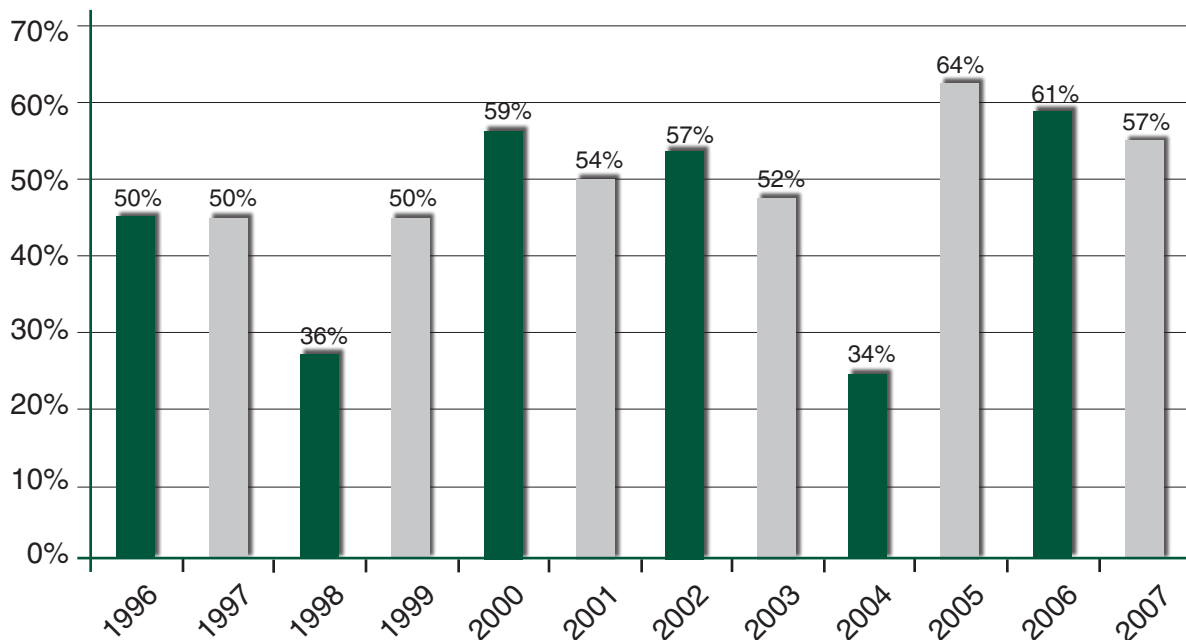
The data reported to ISOO for FY 2007 reveal an estimated 233,639 original classification decisions. These decisions represent a one percent increase (1,644) from data reported in FY 2006. However, the historical timeline chart above indicates a 54 percent decrease to its present level from 507,794 in 1989, and the annual average since E.O. 12958, as amended, was enacted in 1995 is 234,539.

For the third year in a row, the majority of original classification decisions have been assigned a declassification date of ten years or less. In FY 2007, the ten-year-or-less declassification instruction was used 57 percent of the time, which is slightly lower than the 61 percent reported in FY 2006. This pattern indicates that OCAs are not automatically defaulting to a 25-year declassification date, which is the maximum duration that an OCA can apply.

## Duration of Original Classification, FY 2007



## Use of the "Ten Years or Less" Declassification Category



## Derivative Classification

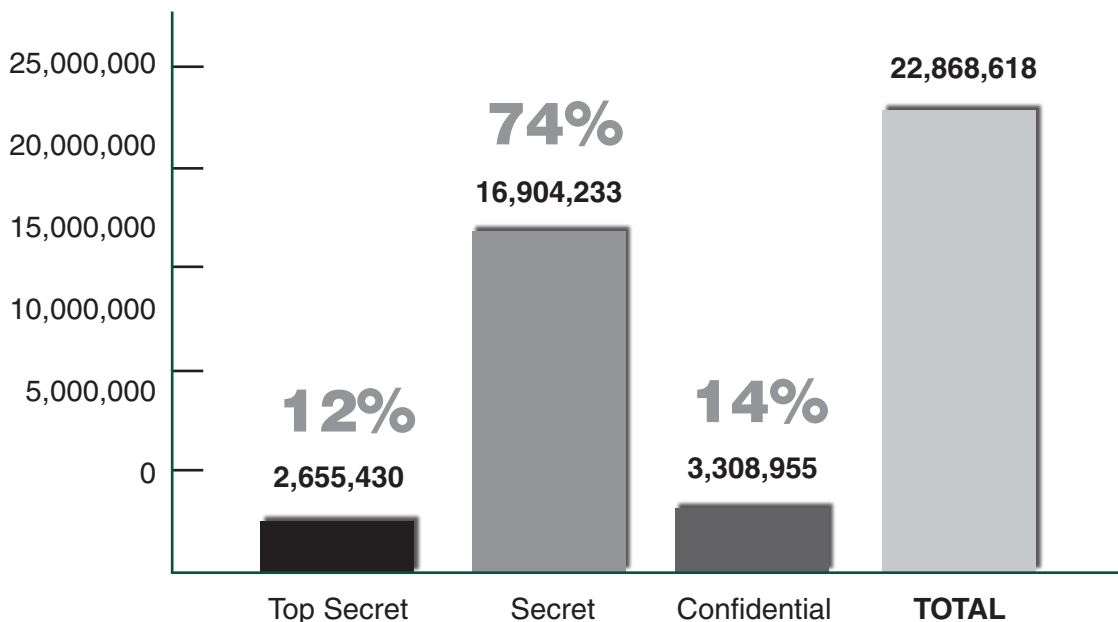
**D**erivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified. Information may be classified in two ways: (1) through the use of a source document, usually correspondence or publications generated by an OCA; or (2)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

to restate classified source information, may classify derivatively.

Derivative classifications reutilize information from the original category of classification, and they may also utilize the same classified elements of information in a variety of formats and venues. Since every derivative classification action is based on information whose classification has already been determined, it is essential that the origin of these actions be traceable to a decision by an OCA.

The agencies reported a total of 22,868,618 derivative classification actions which is a 12.5 percent increase over the 20,324,450 derivative actions reported in FY 2006. This number has steadily increased from the 5,684,462 derivative actions reported for FY 1996, the first full fiscal year following the issuance of E.O. 12958.

### Derivative Classification Activity, FY 2007





## Combined Classification

**T**ogether, original and derivative classification decisions make up what ISOO calls combined classification activity. In FY 2007, combined reported classification activity totaled 23,102,257 decisions. The average combined classification activity since FY 1996 is 12 million actions per year. From FY 1980 through FY 1995, the fiscal year that E.O. 12958 was issued, the annual average for combined classification was 11.5 million decisions per year.

## Why are the Numbers Going Up?

**T**he number of reported combined classification decisions has risen each year. In FY 2005, the combined classification number was 14,206,773. This increased in FY 2006 to 20,556,445 and then to 23,102,257 in FY 2007. The increase, in large part, likely reflects changes in how classified information is generated and used and the resulting complexities of what to report as a classification decision.

When agencies first began reporting the number of their classification decisions,

the ways in which our Government and its contractors produced and disseminated classified information were very different. After the advent of e-mail on classified networks led to some initial confusion over what to report as a classification decision, ISOO stressed the established policy of counting only finished products for retention or dissemination.

In recent years, methods of communicating electronically have expanded significantly. Today, there is even more classified e-mail, as well as many other methods of disseminating and communicating classified national security information, including classified web pages, blogs, wikis, bulletin boards, instant messaging, etc. The accurate assessment of the number of classification decisions has become a complex undertaking.

During FY 2007, ISOO initiated an ongoing effort with representatives of the Executive branch agencies to develop guidance for applying the marking requirements of E.O. 12958, as amended, and 32 C.F.R. Part 2001.30 (the Directive) to the electronic products mentioned above. As this effort continues in FY 2008, we will also consider enhanced guidance to agencies on reporting classification decisions.

# DECLASSIFICATION

---

## Background

**S**ection 3 of E.O. 12958, as amended, establishes three pillars for the Executive branch declassification program: automatic declassification, systematic declassification, and mandatory declassification review (MDR). Under the automatic declassification provisions of E.O. 12958, as amended, records containing classified national security information appraised as having permanent historical value are automatically declassified at 25 years of age unless an agency head has determined that the information falls within a narrow exemption that permits continued classification and either the President or the ISCAP has approved its continued classification. E.O. 12958, as amended, also requires all agencies with original classification

authority to create and maintain a viable systematic declassification program that ensures a declassification review of permanently valuable records that were previously exempted from declassification. E.O. 12958, as amended, further requires agencies to prioritize this review based on researcher interest and the likelihood of declassification. In practice, agencies have conducted this review in advance of the potential onset of automatic declassification, combining both programs into a single review. As a result, the declassification data ISOO has collected during FY 1996 – FY 2007 does not distinguish between the two programs because they have been so interrelated. Finally, the MDR provision of E.O. 12958, as amended, allow the public to request that specific classified information be reviewed for declassification and provides that denials may ultimately be appealed to the ISCAP. All three of these programs are essential in ensuring the continued integrity and effectiveness of the classification system. These programs ensure that there is an ongoing process to purge yesterday's secrets that no longer require protection. It is also through this

process that our Government can ensure the proper protection of information, the release of which reasonably could still be expected to cause damage to our national security. But these programs are also a representation of the vital components of our democracy, one of which is an open society in which the American public, informed by a free flow of information, holds the Government accountable for its actions.

When signed in 1995, E.O. 12958, as amended, served as the impetus for many agencies to devote necessary resources for the establishment of declassification review programs. E.O. 12958 and

---

**These programs ensure that there is an ongoing process to purge yesterday's secrets that no longer require protection.**

---

its 2003 amendment mandate that agencies ensure that all three declassification programs required by the President continue to function effectively. The first major deadline in

E.O. 12958, as amended, has passed. On December 31, 2006 all permanently valuable classified records aged 25 years or older that were not otherwise appropriately exempted, or appropriately excluded, referred, or delayed, were automatically declassified. Now, however, this automatic declassification deadline will repeat itself each year on December 31, as new permanently valuable classified records reach 25 years of age. Following the first automatic declassification date of December 31, 2006, agencies continued to review records becoming eligible for automatic declassification and on December 31, 2007, the second wave of permanently valuable records aged 25 years were subject to automatic declassification. Based on an evaluation of agency data submissions for this fiscal year, it appears that agencies met the requirements of E.O. 12958, as amended, resulting in the declassification of 37.2 million pages. As automatic declassification continues yearly with new records becoming 25 years old, agencies must continue to sufficiently staff and manage their declassification programs. In addition, now that records have been exempted from

automatic declassification, agencies must also begin to focus on and direct resources for the processing and re-review of previously identified exempted records as required by the systematic declassification provisions of the E.O. 12958, as amended.

There are two other major deadlines in E.O. 12958, as amended, which are approaching. First, agencies have been granted a three-year delay in the automatic declassification of records containing classified information from more than one agency. The 2003 amendment to E.O. 12958, as amended, directs agencies to refer these records to appropriate agencies for review but establishes a maximum three-year time frame during which the agencies are to coordinate and complete this review. The initial three-year period will end on December 31, 2009. As will be discussed below, ISOO is concerned about agencies' progress in this area. Second, E.O. 12958, as amended, grants agencies a five-year delay in the automatic declassification of classified national security information contained in microforms, motion pictures, audio tapes, videotapes, or comparable media. E.O. 12958, as amended, recognizes that conducting a declassification review of these "special media" records could be more costly, difficult, or time-consuming and allows agencies to delay automatic declassification. The grace period for these "special media" records ends on December 31, 2011. Agencies are expected to utilize this five-year delay to develop policies and procedures to account for these "special media" challenges and to process these records. Although some agencies are taking steps to consider their "special media" records, others are not. Addition-

ally, agencies have not focused on how to process referrals of "special media" records. Instead, agencies are continuing their agency-centric declassification approach and are focusing more on how to best review the massive number of textual referrals in anticipation of the December 31, 2009 deadline.

## The Looming Issue of Referrals and the December 31, 2009 Deadline

Section 3.3(e)(3) of E.O. 12958, as amended, states that "before the records are subject to automatic declassification, an agency head or senior agency official designated under section 5.4 of E.O. 12958, as amended, may delay automatic declassification for up to three years for classified records that have been referred or transferred to that agency by another agency less than three years before automatic declassification would otherwise be required." Thus, E.O. 12958, as amended, provides agencies with limited relief and an opportunity to delay the onset of automatic declassification of 25 year old (or older) permanently valuable records containing classified national security information of multiple agencies. For records referred by December 31, 2006, the delay in processing these referrals ends on December 31, 2009. Agencies are fully expected to complete their review by this deadline. In order to qualify for the three-year delay, agencies were required to have referred those records containing classified information of other agencies by December 31, 2006. Agencies receiving the referred records then have extra time to





conduct a declassification review and provide their decisions to the original referring agency. Based on the data ISOO has received, agencies by and large have referred records to other agencies as required by E.O. 12958, as amended. But, in evaluating the increasingly large number of referrals, the progress of agencies to date, and in looking at agency resources dedicated to reviewing referrals, ISOO has concerns about the agencies meeting their responsibilities under E.O. 12958, as amended, and meeting the December 31, 2009 deadline.

In previous Annual Reports, ISOO noted that the current agency-centric approach used by agencies in conducting declassification reviews is problematic when reviewing records containing classified information from multiple agencies. These agency-centric reviews have created millions of records requiring referral to other agencies that must be adjudicated by December 31, 2009. In some cases, agencies reviewing their own records have failed to properly refer classified information from other agencies to those agencies. This has led to records being designated as declassified improperly. Unfortunately, agencies that properly should have had the opportunity to review their classified information never were afforded that opportunity. As a result, on a few notable occasions, these agencies took steps to remove records from public access, in effect reclassifying them. Conversely, in many other cases, agencies have simply referred any and all information from other agencies to other agencies without discrimination. These inappropriate referrals have led to a “mountain” of records requiring unnecessary review, as the information was either not sensitive in the first place, or is no longer sensitive.

## FY 2008 ISOO Assessments

**A**s part of its oversight responsibilities, in FY 2008, ISOO will evaluate and assess agency automatic declassification reviews. These assessments will focus on three potential problem areas within the automatic declassification review process: missed equities (where the reviewing agency responsible for conducting the automatic declassification review failed to properly refer clas-

sified information belonging to other agencies); inappropriate referrals (where the reviewing agency responsible for conducting the automatic declassification review referred information to other agencies that either should never have been referred in the first place as the information was clearly not sensitive, or should not have been referred to a particular agency as that agency had no equity or interest in the information); and inappropriate exemptions from declassification. ISOO intends to conduct these assessments annually and, beginning in FY 2010, report the results in the Annual Report to the President. In conducting these reviews, ISOO will analyze the results, capturing both problematic areas and best practices, and use the results to recommend specific programmatic improvements for individual agencies and for the overall declassification program.

## Pages Reviewed and Pages Declassified

**D**uring FY 2007, the Executive branch reviewed 59,732,753 pages for declassification and declassified 37,249,390 pages. As will be detailed below, the overall number of pages reviewed by Executive branch agencies has declined slightly while the number of pages declassified has increased from previous years. The Department of Defense (DOD) and the military services Department of the Navy (Navy), Department of the Army (Army), and the Department of the Air Force (Air Force) reviewed 33,466,497 pages, or 56 percent of the total number of pages reviewed by all Executive branch agencies. Additionally, DOD and the three military services accounted for 64 percent of the total number of pages declassified. Of the 37.2 million pages declassified by Executive branch agencies, DOD and the three military services declassified 23,888,287 pages. Although Navy experienced an 11 percent decrease in the number of pages reviewed this fiscal year compared with last year, they led all Executive branch agencies by reviewing a total of 11,818,797 pages. In addition, Navy also declassified 8,289,660 pages, the highest total amount in the Executive branch.



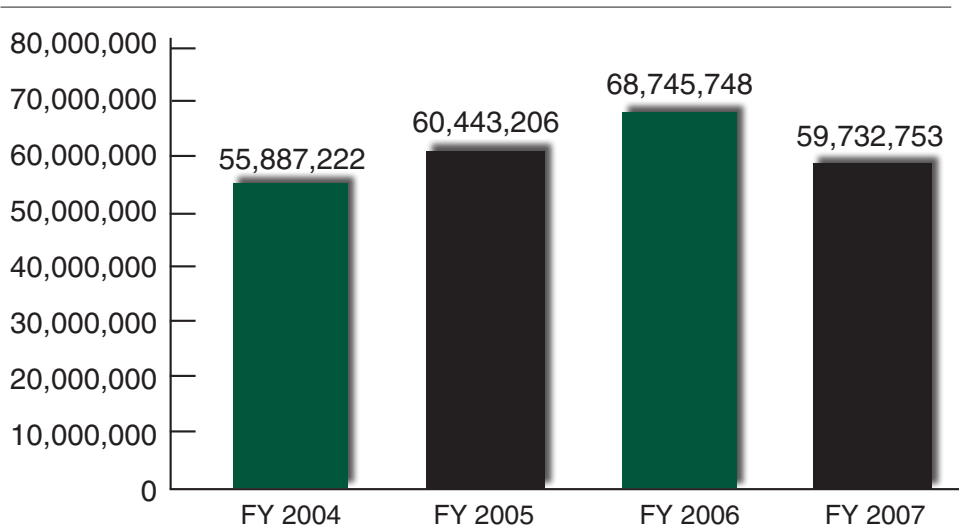
In FY 2004, ISOO required agencies to begin reporting the number of pages reviewed in addition to the number of pages declassified. The intent was that this number would provide a better understanding of the total level of effort. With the FY 2007 data, ISOO now has four years of data for comparison. In FY 2004, the Executive branch agencies reviewed 55,887,222 pages; in FY 2005, this number increased by 8 percent to 60,443,206; and, in FY 2006 this increased again, this time by 14 percent to 68,745,748. Now, in FY 2007, after two years of steady increases in the number of pages reviewed, there was a 13 percent decrease. This could be explained by the fact that records older than 25 years as of December 31, 2006, were processed for declassification in anticipation of that date, or were otherwise automatically declassified. Thus, in FY 2007, agencies were reviewing only records that were created in 1982, reaching 25 years of age by December 31, 2007, rather than the much larger universe that encompassed anything created prior to 1982, such as was done during previous years. Consequently, many agencies saw significant decreases this fiscal year. For example, the Department of Commerce experienced a substantial decrease, from 1.6 million pages reviewed in FY 2006 to 10,983 pages reviewed in FY 2007. In addition, the Department of Justice (Justice), to include the Federal Bureau of Investigation (FBI), experienced a 92 percent decrease

(from 11,202,456 pages reviewed in FY 2006 to 947,101 pages in FY 2007). The Department of Energy (DOE), (86 percent decrease) and the National Aeronautics and Space Administration (NASA), (30 percent decrease) also experienced significant decreases from FY 2006. Still, the number of pages reviewed through the automatic and systematic declassification programs increased by approximately 7 percent from the FY 2004 baseline figure.

During FY 2007, the Executive branch declassified 37,249,390 pages of permanently valuable historical records, which is a decrease of 1 percent from the 37,647,993 pages declassified in FY 2006. Importantly, while the number of pages declassified has basically remained unchanged from FY 2006, the declassification rate has steadily increased. The FY 2007 numbers reveal that agencies are now declassifying 62 percent of the materials they review. This represents a 7 percent increase from FY 2006 when agencies were declassifying close to 55 percent of the records reviewed. In FY 2005, the declassification rate was 52 percent. In FY 2004, the first year ISOO began tracking this data, it was 51 percent.

In FY 2007, the Department of Defense and the three military services had a combined declassification rate of 71 percent. The Air Force had the highest rate within DOD, 83 percent, while the Army had the lowest, 47 percent. Both of these services saw increases in their declassification rate

### Total Number of Pages Reviewed

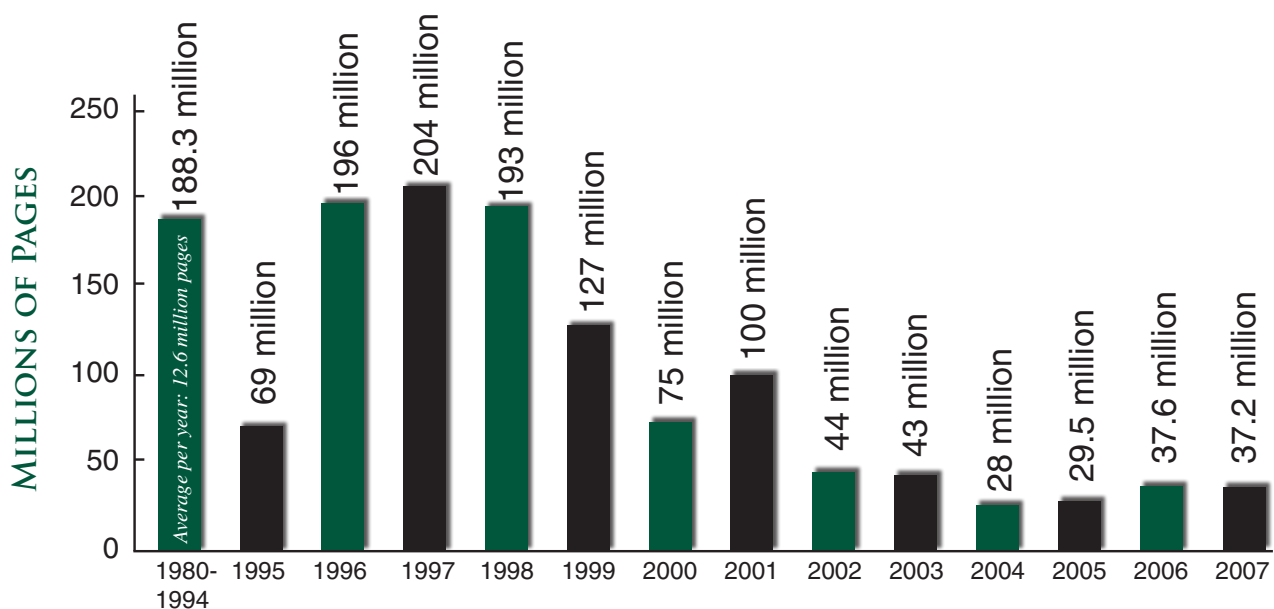


from FY 2006: the Air Force improved its declassification rate by 21 percent (FY 2006: 62 percent) and the Army achieved an 8 percent increase (FY 2006: 39 percent). The Navy's declassification rate dropped by 4 percent from 74 percent in FY 2006 to 70 percent in FY 2007.

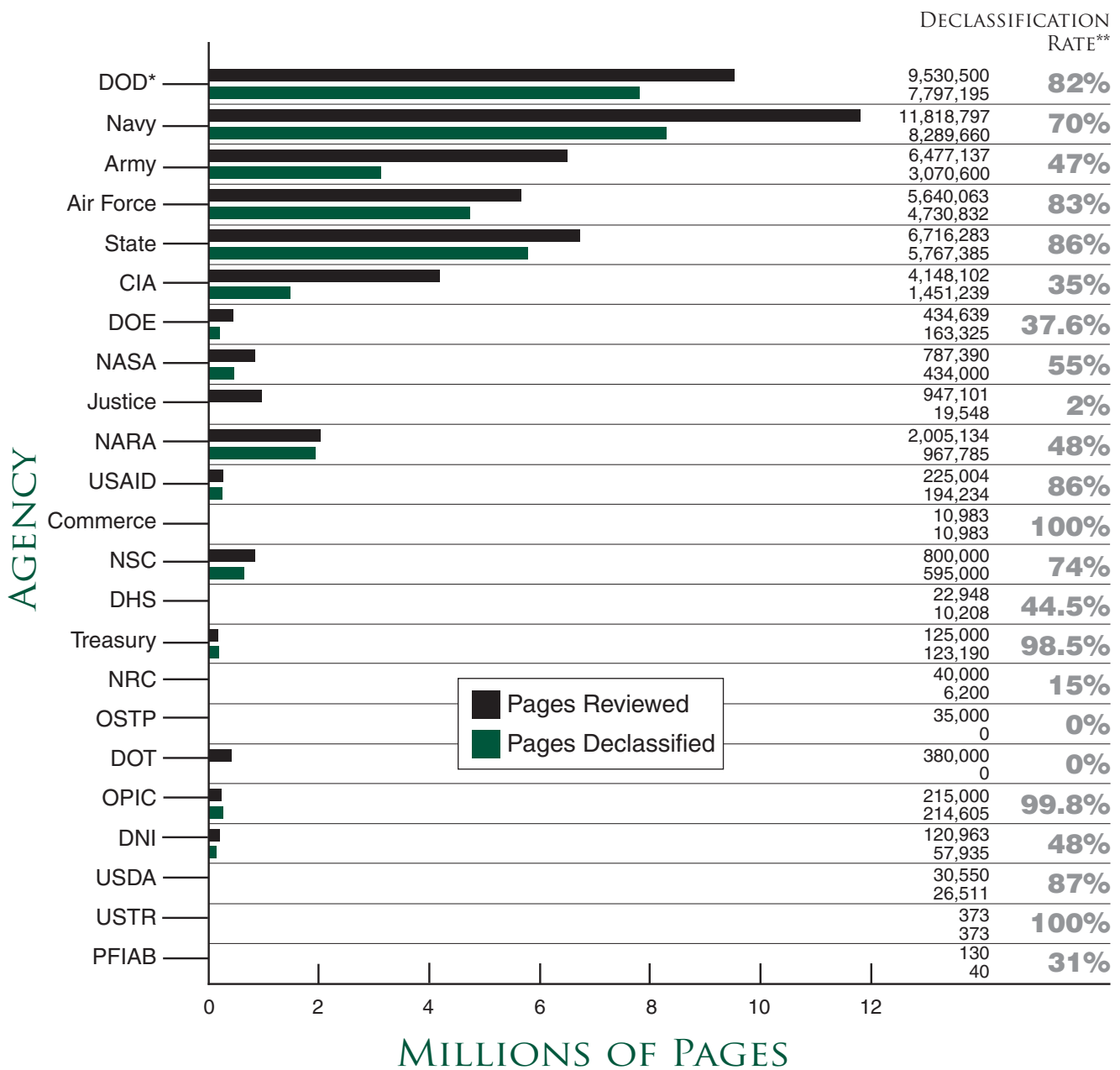
Both the National Security Council (NSC) (1043 percent) and the National Archives and Records Administration (NARA) (112 percent) had notable increases in the number of pages reviewed in FY 2007 compared with their FY 2006 statistics and had corresponding increases in the number of pages declassified. The NSC declassified 595,000 pages in FY 2007 (1044 percent increase from FY 2006) and NARA declassified 967,785 pages (350 percent increase from FY 2006). NARA achieved a 48 percent declassification rate in FY 2007, an improvement of 25 percent from FY 2006 (23 percent). In FY 2007, the Department of State (State) reviewed 6,716,283 pages for automatic declassification, representing a 25 percent increase from FY 2006. Their declassification rate improved from 85 percent in FY 2006 to 86 percent in FY 2007 as they declassified a total of 5,767,385 pages.

The Central Intelligence Agency (CIA) reviewed 4,148,102 pages in FY 2007, a 138 percent increase from FY 2006 when they reviewed 1,744,315 pages. However, this large increase did not result in a corresponding large increase in the number of pages declassified in FY 2007. In FY 2006, they declassified 1,021,105 pages and in FY 2007, they declassified 1,451,239 pages. In fact, CIA's declassification rate experienced a significant decrease of 23 percent from 58 percent in FY 2006 to 35 percent in FY 2007. In FY 2007, Justice, to include the FBI, reviewed 947,101 pages for automatic declassification and declassified 19,548 pages, or 2 percent. Although the 2 percent declassification rate is low, this is a slight increase in the declassification rate from FY 2006 when Justice reviewed 11,202,456 pages and declassified 153,333 pages (a declassification rate of 1.4 percent). Two agencies did not declassify any pages during FY 2007: the Office of Science and Technology Policy (which reviewed 35,000 pages) and the Department of Transportation (which reviewed 380,000 pages). These two agencies have referred classified national security information to other agencies for declassification review.

### 1.37 Billion Pages Declassified, FY 1980 - FY 2007



## Number of Pages Reviewed and Declassified by Agency, FY 2007



**TOTAL:** 59,732,753 pages reviewed  
 37,249,390 pages declassified  
**62%** declassification rate

\*Less Army, Navy, and Air Force

\*\* It is important to point out that at several agencies the bulk of the records requiring review contain information originated by other agencies. Therefore, the bulk of the records must be referred to those agencies for declassification determinations.

## Mandatory Declassification Review

Under E.O. 12958, as amended, the Mandatory Declassification Review (MDR) process permits individuals or agencies to require the review of specific classified national security information for the purpose of seeking its declassification. Requests must be in writing and must describe the document or material containing the information with sufficient specificity to permit the agency to locate it with a reasonable amount of effort. MDR remains popular with some researchers as a less litigious 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.

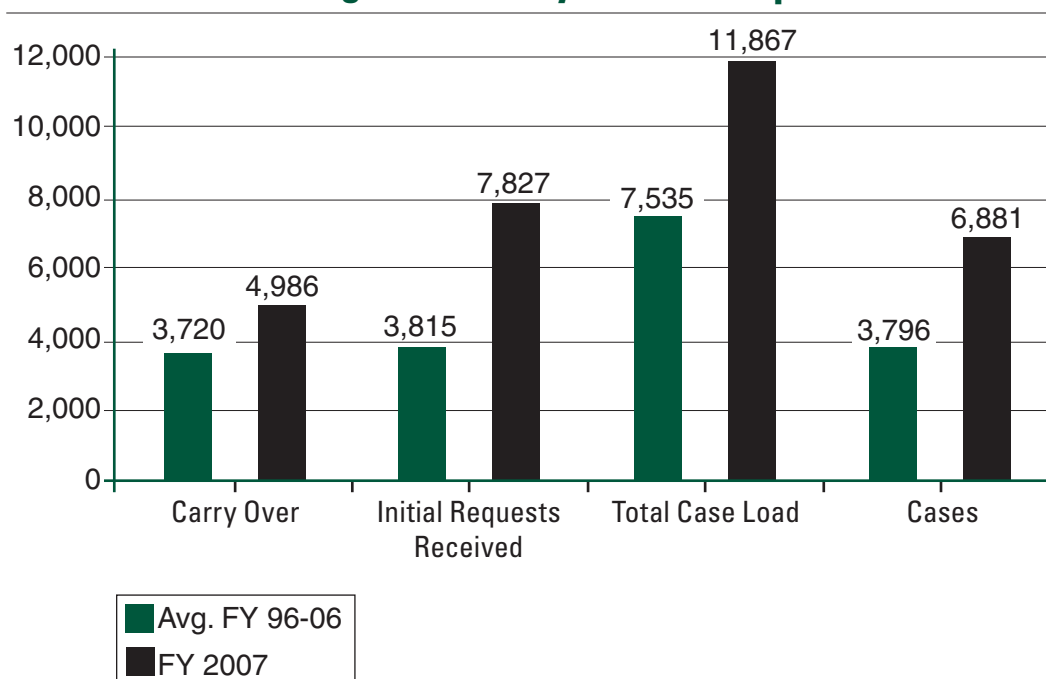
### Initial Requests

Agencies received 7,827 new initial requests and processed 6,881 initial requests for MDR during FY 2007. This represents a dramatic increase in initial requests from FY 2006 when agencies received 3,769 MDR requests and

processed 3,378 requests. The total number of pages processed during FY 2007 was 461,496. This is also a dramatic increase from FY 2006 when agencies processed 123,469 pages. This means that in FY 2007, agencies processed 338,027 more pages than in FY 2006. For FY 2007, three agencies accounted for 89 percent of the new initial requests: DOD and the military services (4,733 requests), CIA (1,213 requests), and NARA (1,029 requests). These same three agencies also accounted for 89 percent of the pages reviewed and processed for MDR in FY 2007. DOD accounted for 70 percent (323,588 pages) while the CIA accounted for 12 percent (56,106 pages), and NARA accounted for 7 percent (30,234 pages).

In analyzing the historical data between FY 1996 and FY 2007, it is apparent that MDR has become a more popular forum for the public to use in requesting declassification reviews for records. There are several reasons for this. First, researchers have greater understanding of the benefits of using MDR. As will be discussed later in this section, on average, information is declassified in 91 percent of the pages reviewed. Second, researchers

### MDR Program Activity - Initial Requests



have greater understanding of agencies' records systems (and therefore can make specific requests for records still in agencies' custody). Additionally, the number of initial MDR requests submitted to agencies will likely increase as researchers begin to request individual records that had been exempted from declassification during the automatic and systematic declassification review processes.

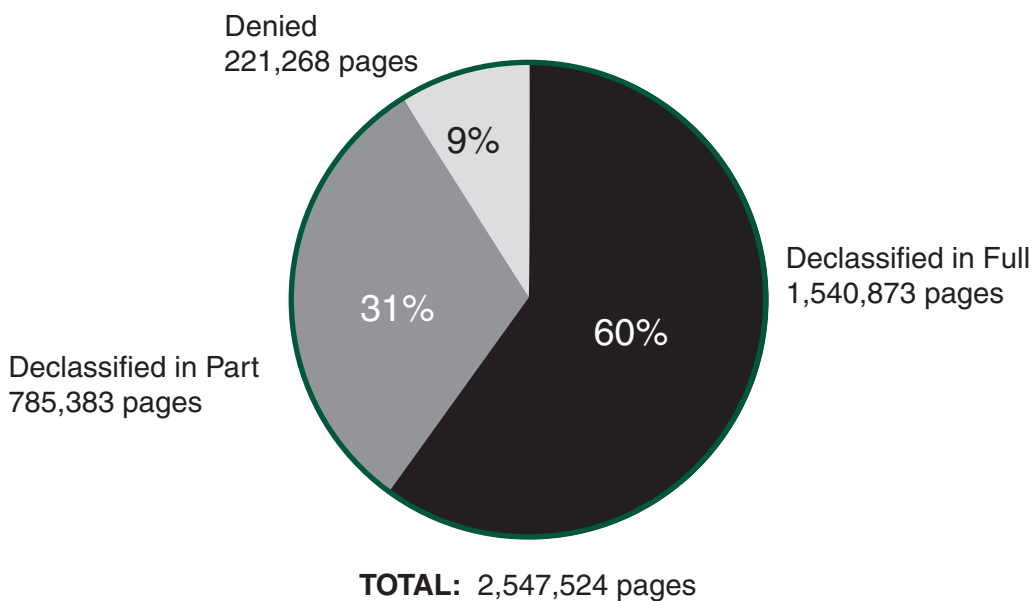
As the data indicates, FY 2007 was a record-setting year for MDR programs. In aggregate, agencies received their highest number of initial requests. Between FY 1996 and FY 2006, agencies received an average of 3,815 initial requests per year. This figure increased by 105 percent in FY 2007 as agencies received 7,827 new requests. In addition, agencies processed a record number of cases and reviewed a record number of pages. Historically, agencies processed an average of 3,796 cases per year between FY 1996 and FY 2006. This figure increased significantly (81 percent) in FY 2007 as agencies processed 6,881 cases. The most dramatic increase, however, has been in terms of the number of pages reviewed. On average, agencies reviewed 189,680 pages each fiscal year during this same

time period (FY 1996 to FY 2006). In FY 2007, this number increased by 143 percent as agencies reviewed 461,496 pages.

ISOO remains concerned about the size of the backlog of initial requests carried over from fiscal year to fiscal year. On average, from FY 1996 to FY 2006, agencies annually carried over 3,720 cases into the next fiscal year. For FY 2007, agencies carried over 4,986 initial requests into FY 2008. In evaluating the overall MDR statistics from FY 1996 through FY 2006, agencies carried over an average of 50 percent of their total case load from one fiscal year to the next. In FY 2007, this figure improved slightly. Agencies are carrying over into FY 2008 just over 42 percent of the total case load.

In FY 2006, four agencies accounted for the majority of requests carried over from FY 2006 into FY 2007. They were: DOE (243 requests), DOD and the military services (530 requests), CIA (706 requests), and NARA (1,714 requests). When combined, these four agencies accounted for 97 percent of the entire backlog of initial MDR requests. For FY 2007, only DOE has made progress in eliminating the size of its backlog. They have decreased the size of their backlog by 44 percent

### Disposition of Initial MDR Requests, FY 1996 - FY 2007



and are only carrying over a backlog of 161 requests into FY 2008. The CIA backlog remained essentially the same, as they are carrying over 705 requests. NARA has the largest backlog. They are carrying over 2,060 initial requests into FY 2008, a 17 percent increase from the previous fiscal year. NARA's case backlog alone accounted for 49 percent of the total backlog figure for all agencies. DOD also had a significant increase in its backlog. For FY 2008, DOD doubled its backlog from the previous fiscal year and is carrying over 1,067 initial requests. Three other agencies reported carrying over notable backlogs of initial requests into FY 2008. They were: the Department of Homeland Security (114 requests), State (59 requests) and Justice (40 requests).

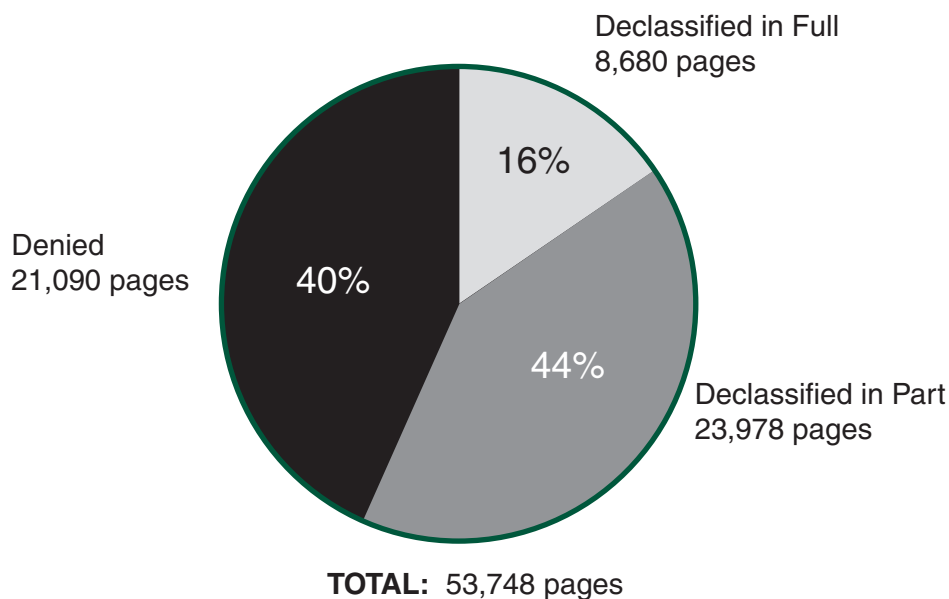
The processing of initial requests for MDR during FY 2007 resulted in the declassification of information in 431,371 pages, or 93 percent of the pages reviewed. Specifically, it resulted in the declassification of 347,338 pages in full (75 percent) and 84,033 pages in part (18 percent). 30,125 pages (7 percent) remained classified in their entirety after being reviewed. Historically, since FY 1996, agencies have reviewed 2,547,524 pages under the MDR process. Agencies have declassified informa-

tion in 91 percent of the pages processed from FY 1996 – FY 2007. Only 9 percent were denied in full. In FY 2007, the percentage of pages declassified in full (75 percent) was significantly better than the historical average (60 percent). The percentage of pages denied in full in FY 2007 (7 percent) was slightly less than the 9 percent historical average.

## Appeals

**D**uring FY 2007, agencies processed 104 appeals of agency decisions to deny information during the processing of initial requests for MDR. This represents a significant increase from FY 2006, when agencies only processed 67 MDR appeals, but is slightly below the overall average of 106 appeals processed annually for the period FY 1996 through FY 2006. Agencies face a continuing and growing backlog of MDR appeals. According to agency data, 105 appeal cases are being carried over to FY 2008; NARA (42 cases), CIA (31 cases), and DOD (20 cases) account for nearly the entire backlog of appeals. These agencies need to give additional attention to ensure that they are meeting their responsibilities in this area. However, as noted in our last Annual Report, ISOO is particularly con-

### Disposition of MDR Appeals, FY 1996 - FY 2007





cerned about MDR appeals processing at NARA. NARA closed 23 appeals in FY 2005 and closed 6 appeals in FY 2006. In FY 2007, NARA closed 11 appeals and is carrying over 42 appeals into FY 2008, the highest number of any agency. NARA has committed to a special effort during FY 2008 to reduce its backlog of MDR appeals.

Agencies reviewed 8,122 pages as part of these MDR appeals, representing a sizeable increase from the 5,558 pages reviewed in FY 2006. The processing of MDR appeals by agencies during FY 2007 resulted in the declassification of information in 5,346 pages, or 66 percent of the pages reviewed. Specifically, it resulted in the declassification of 1,285 pages in full (15 percent) and 4,067 pages in part (50 percent). 45 percent, or 2,776 pages, remained classified in their entirety after being reviewed.

Additional 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 then be appealed by the requester directly to the ISCAP. 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.

An ISOO special review of the MDR program in Executive branch agencies, which was outlined in ISOO's FY 2005 Annual Report, revealed the need for a better understanding of MDR requirements and procedures. Therefore, in FY 2006 ISOO hosted an MDR workshop for public and Government participants that focused on the rights of a requestor and the responsibilities of Government agencies. ISOO continued this type of training in FY 2007 and intends to provide additional

MDR training sessions in FY 2008.

While it is too early to tell whether the FY 2007 statistics represent simply a spike or a fundamental shift and increase in the use of MDR, ISOO intends to monitor agency MDR programs carefully in the forthcoming years. Agencies must also evaluate their own MDR programs and, should the situation warrant, be prepared to devote sufficient resources to this program to account for these increases. Finally, for those agencies carrying over large case backlogs from one fiscal year to the next, they must take steps to eliminate the backlogs. Compliance with the MDR provisions of E.O. 12958, as amended, is not optional. Section 3.5 of E.O. 12958, as amended, requires agencies to create, staff, and maintain viable and effective MDR programs. The issuance of E.O. 13392, "Improving Agency Disclosure of Information," on December 14, 2005, has been the basis for confusion on the part of some agency representatives. They have informally pointed to the requirements of E.O. 13392 and its focus on the requirements of the FOIA when addressing their compliance with the MDR requirements. This rationale is incorrect. E.O. 13392 has no effect on the MDR provisions of E.O. 12958, as amended. Agencies must comply with all of the requirements of both MDR and FOIA and commit the necessary resources to ensure the effective implementation of both.

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: [www.archives.gov/isoo/oversight-groups/iscap/mdr-appeals.html](http://www.archives.gov/isoo/oversight-groups/iscap/mdr-appeals.html)

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

Telephone: 202.357.5250

Fax: 202.357.5907

E-mail: [iscap@nara.gov](mailto:iscap@nara.gov)



## Audit of the Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes

In 2006, under the provisions of E.O. 12958, as amended, and in response to a request from the Archivist of the United States, as well as a group of concerned individuals and organizations, ISOO performed an audit of all re-review efforts undertaken since 1995 by agencies in their belief that certain records at NARA had not been properly reviewed for declassification, but had been made available to the public. The full audit report can be found online at: <http://www.archives.gov/isoo/reports/2006-audit-report.html>

Although over two years have passed since ISOO conducted its audit and the agencies involved in the withdrawals and NARA have agreed to prioritize the re-review efforts to return as many withdrawn records to the public shelves as quickly as possible, not all records have been processed. At the end of FY 2007, some agencies, including the CIA and Air Force, had yet to complete their reviews and return their decisions to NARA. At the conclusion of FY 2007, over 5,000 referrals to agencies had yet to be adjudicated. Additionally, as of the end of the fiscal year, NARA had not yet acted on all agency decisions it had received. ISOO had hoped to provide a full accounting of the audit, but, as there are still significant outstanding issues, this final report must wait until all work has been completed, including the final adjudication of all referrals and the return of all declassified records to the open shelves for public access. In discussions with agencies on this matter, ISOO has noted that agencies have made a significant effort to complete this important project. They have made progress and they are committed to resolving all remaining issues in FY 2008.

## Subsequent Reclassification Activity at NARA

As noted in the Audit Report, increased transparency would help ensure that any future withdrawal actions would occur only when absolutely necessary in the national interest. Also, it could dispel perceptions that such efforts are attempts to conceal official embarrassment or to otherwise attempt to “rewrite history.” As a result of this audit, the affected agencies initially agreed to abide by interim guidance that includes provisions that require the public to be informed that records have been formally withdrawn from public access at NARA due to classification action, as well as how many records are affected. This interim guidance, titled “Interim Guidelines Governing Re-review of Previously Declassified Records at the National Archives,” is available online at: [www.archives.gov/isoo/reports/2006-audit-report-attach-2.pdf](http://www.archives.gov/isoo/reports/2006-audit-report-attach-2.pdf)

While it is awaiting final promulgation as a change to 32 C.F.R. Part 2001.13, the interim guidance remains binding on all agencies. The interim guidelines are having the desired effect. In accordance with the public notification provision of this guidance, agencies reported only three such actions in FY 2007. The Air Force withdrew two records totaling two pages, and DOE withdrew one document totaling seven pages. Each of these actions occurred in the first two quarters of the fiscal year. This stands in stark contrast to the previous withdrawal activity. However, ISOO will continue to monitor such activity closely, and continue to report publicly on all future withdrawal actions.

# INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

---

## Authority

Section 5.3 of E.O. 12958, as amended, “Classified National Security Information.”

## Functions

1. To decide on appeals by authorized persons who have filed classification challenges under section 1.8 of E.O. 12958, as amended.
2. To approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of E.O. 12958, as amended.
3. To decide 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

Mark A. Bradley  
Department of Justice

Edmund Cohen  
Central Intelligence Agency

Margaret P. Grafeld  
Department of State

Robert Andrews  
Department of Defense

Michael J. Kurtz  
National Archives and Records Administration

## Executive Secretary\*

J. William Leonard, Director  
Information Security Oversight Office

\*The individuals named in this section were those in such positions as of the end of FY 2007.

## Support Staff

Information Security Oversight Office

## Summary of Activity

**T**he ISCAP was created under E.O. 12958 to perform the critical functions noted above. The ISCAP, comprised 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 ISOO serves as its Executive Secretary; and ISOO provides its staff support.

## Declassification Guides

**D**uring FY 2007, the ISCAP continued to review declassification guide submissions from Executive branch agencies in accordance with section 3.3(d) of E.O. 12958, as amended, and the applicable provision of its Government-wide implementing directive (32 C.F.R. Part 2001.30(j)). 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 3.3(b) of E.O. 12958, as amended. 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 FY 2007, the ISCAP received 22 declassification guide submissions. This number included new submissions, updates to previously

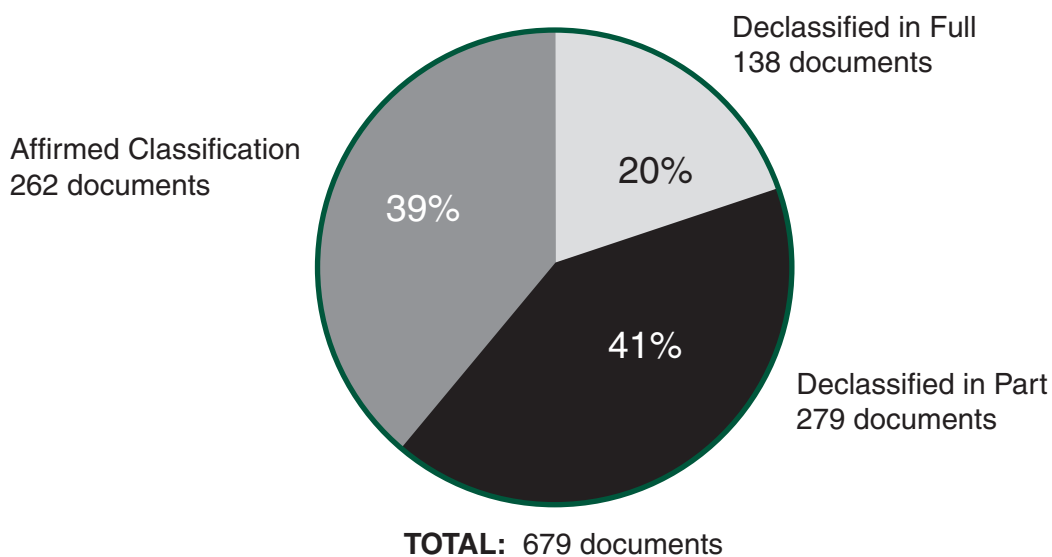
approved guides, and instances in which agencies requested permission to utilize the approved guide of another agency. By the end of FY 2007, the ISCAP had reviewed each submission, provided the agencies with comments and suggestions, received and reviewed revised versions from the agencies, and approved 18 declassification guide submissions. Specifically, the ISCAP issued final approval for the declassification guide submissions of: Air Force; Army; two guides for DHS, one for the Federal Emergency Management Agency and one for the United States Secret Service; DOE; three guides for Justice, one for the Office of Information and Privacy, one for the Office of Intelligence Policy and Review, and one for FBI; the Defense Threat Reduction Agency; the Missile Defense Agency; the National Geospatial-Intelligence Agency; the Nuclear Regulatory Commission; two guides for the Office of the Secretary of Defense, a general one and one specific to the Defense Continuity Program. The ISCAP also issued temporary, interim approvals for the guides submitted by the Air Force Technical Applications Center and the National Security Agency, with final approval

pending. Additionally, the ISCAP approved the Office of the Director of National Intelligence to utilize the previously approved Central Intelligence Agency declassification guide and the Unified Combatant Commands to utilize the previously approved Joint Chiefs of Staff declassification guide.

## Mandatory Declassification Review Appeals

As noted above, the ISCAP expended significant effort during FY 2007 to consider agency declassification guide submissions. This limited the time available for the consideration of mandatory declassification review appeals. In FY 2007, the ISCAP decided upon 24 documents that remained fully or partially classified following requests lodged under the mandatory declassification review provisions of E.O. 12958, as amended. It declassified information in 17 percent of the documents that it decided upon, declassifying the entirety of the remaining classified information in one document (four percent) and declassifying some portions while affirming the classification of

### ISCAP Decisions, May 1996 - September 2007



other portions in three of the documents (13 percent). The ISCAP fully affirmed the prior agency decisions in their entirety for 20 documents (83 percent). It should be noted that these 20 documents had been previously reported as declassified in their entirety or in part in the ISCAP section of the FY 2005 ISOO Annual Report and the data likewise carried forward in the FY 2006 ISOO Annual Report. However, the ISCAP decided to delay implementation of its decisions on these documents and then later decided to reverse its decisions on these documents during FY 2007.

From May 1996 through September 2007, the ISCAP decided upon 679 documents. Of these, the ISCAP declassified information in 61 percent of the documents.

Specifically, it has declassified the entirety of the remaining classified information in 138 documents (20 percent) and

declassified some portions while affirming the classification of other portions in 279 documents (41 percent). The ISCAP has fully affirmed agency classification decisions in 262 documents (39 percent).

While the chart on the previous page represents 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 E.O. 12958, as amended, 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.

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.

## Classification Challenges

During FY 2007, the ISCAP heard two appeals of classification challenges filed pursuant to section 1.8 of E.O. 12958, as amended. One appeal sought to reverse the decision of the Secretary of State that 143 specific Diplomatic Telecommunications Service Program Office messages were classified. The ISCAP determined that the documents in question were properly classified in accordance with the standards for classification found in section 1.1 of E.O. 12958, as amended.

The other classification challenge appeal sought to reverse the determination of the Secretary of Defense that information within a January 2005 "Per-

sons Query" printout from a DOD database known as the Joint Detainee Information Management System was classified. The ISCAP determined that the document in question was properly classified in accordance with the standards for classification found in section 1.1 of E.O. 12958, as amended.

## Appeals Concerning ISCAP Decisions

In recognition of the need to hear appeals of agency decisions relating to the MDR program and as 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.

---

**As agencies gain experience with the provisions of the E.O. 12958, as amended, the ISCAP has seen less misapplication of the classification standards.**

---



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 of 1996 through the amendment of E.O. 12958 in FY 2003, this authority had not been exercised by any agency head; the same was true for FY 2004 – FY 2007.

However, with the amendment of E.O. 12958 in FY 2003, the Director of Central Intelligence (DCI) was authorized to block declassification by the ISCAP of certain information owned or controlled by the DCI. Such DCI determinations could be appealed to the President (see section 5.3(f) of E.O. 12958, as amended).

During FY 2003, the DCI blocked the declassification of two documents that the ISCAP had voted to declassify. In both instances, members of the ISCAP appealed the DCI's determination to the President through the Assistant to the President for National Security Affairs. During FY 2004, one of these appeals was rendered moot as the DCI later declassified the document at issue in its entirety.

The second appeal remains pending and as such, the document remains classified in its entirety.

From FY 2004 through FY 2007, the authority under section 5.3(f) of E.O. 12958, as amended, has not been exercised. The Intelligence Reform Act of 2004 established the Office of the Director of National Intelligence and amended the National Security Act of 1947 to strike the DCI from the pertinent portions by replacing the DCI with the Director of National Intelligence (DNI). The authority established with the 2003 amendment to E.O. 12958 and found in section 5.3(f) of E.O. 12958, as amended, now rests with the DNI.

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

Telephone: 202.357.5250

Fax: 202.357.5907

E-mail: [iscap@nara.gov](mailto:iscap@nara.gov)

Additional information about ISCAP may be found on this portion of the ISOO website:  
[www.archives.gov/isoo/oversight-groups/iscap/](http://www.archives.gov/isoo/oversight-groups/iscap/)





## ON-SITE REVIEWS

---

### General Program Reviews

In FY 2007, pursuant to sections 5.2(b)(2) and (4) of E.O. 12958, as amended, ISOO conducted ten on-site reviews of Executive branch agencies. These were general program reviews that evaluated the agencies' implementation of the classified national security information program and covered core program elements, such as program organization and management, classification, security education and training, self-inspections, security violation procedures, safeguarding practices, and classification markings.

Several of the on-site reviews conducted in FY 2007 were of agencies we had reviewed in the last three to five years. With one exception, these agencies made notable progress in addressing deficiencies found in the previous reviews.

Several of the programs were notable, as they effectively implemented nearly all of the core elements of the classified national security information program, but a few had significant deficiencies. Disappointingly, we continued to find deficiencies at multiple agencies relating to basic requirements concerning implementing regulations, security education and training, self-inspections, classification, and document markings. To date, we have provided our findings to the specific agency reviewed for corrective action. During FY 2008, we will seek to identify a means to communicate general areas of concern to all agencies with responsibility for classified national security information.

Fundamental program organization and management requirements are not being met at several of the agencies we reviewed. Four out of ten agencies we reviewed had not updated their regulations that implement E.O. 12958, as amended, as required by section 5.4(d)(2) of E.O. 12958, as amended, despite the passage of four years since it was amended in 2003. Also, despite the requirement of E.O. 12958, as amended, that heads of agencies commit necessary resources to the effective implementation of the program, four

of the agencies had insufficient staff to adequately manage and oversee the classified national security information program. The same agencies did not meet the requirement of E.O. 12958, as amended, to ensure that the performance contract or other system used to rate civilian or military personnel performance include the management of classified information as a critical element or item to be evaluated in the rating of OCAs, security managers or security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information (see section 5.4(d)(7) of the E.O. 12958, as amended). Deficiencies in these areas result in weaknesses throughout the program. Out-of-date regulations are one of the main reasons for the continued use of a marking that was eliminated by the 2003 amendment to the E.O. 12958. Insufficient security staff is a direct cause of the failure of some agencies to implement essential program elements, such as security education and training and self-inspections.

During our general program reviews in FY 2007, ISOO continued to concentrate on the appropriateness of classification decisions. We focused on evaluating whether agencies were correctly applying the standards of E.O. 12958, as amended, for the original and derivative classification of information, the fundamental reason for the existence of the classified national security information program. Unfortunately, we continued to find weaknesses in this core element. The appropriateness of classification was subject to question in almost 20 percent of the 1,873 documents we reviewed this year. More than 16 percent of the documents did not contain either a "Classified By" line or a "Derived From" line. Without this information, it is not possible to readily determine if the information is properly classified. Original classification decisions can only be made by an OCA, who must be identified on the document, and derivative classifications must cite their source document(s) or a classification guide, which would allow derivative classifications to be traced to a proper original classification decision. Similarly,

for those instances of derivative classification based on multiple sources that lacked the required list of source materials with or on the official file or record copy of the document (3.4 percent of the documents), it was not possible to track these classification decisions to their source documents. Documents must properly cite the basis for classification, both to protect the integrity of the classification system and the security of the information.

The majority of the agencies we reviewed were deficient with regard to the utilization of security classification guides. Three agencies with OCA have been repeatedly classifying the same categories of information through OCA decisions, instead of preparing security classification guides to facilitate the proper and uniform derivative classification of the information, as required by section 2.2 of E.O. 12958, as amended. Another agency could not identify the classification guides that were currently in use at the agency, and still another had not reviewed and updated its guides as circumstances require and at least once every five years, as required by section 2001.15 of ISOO Directive No. 1. The use of outdated classification guides was noted in our annual report last year and, along with out-of-date agency implementing regulations, continues to be one of the main reasons for the continued application of the obsolete X1–X8 declassification markings, which were eliminated by the 2003 amendment to E.O. 12958.

Section 1.8 of E.O. 12958, as amended, specifies that 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. At two agencies we reviewed, some personnel were unaware of this provision. We have reminded the agencies we reviewed and the personnel we interviewed of this procedure that addresses the possibility that information may be improperly classified or unclassified and noted that training on this topic is among the required elements of initial training.

Several agencies did not meet the security education and training requirements of E.O. 12958, as amended, and ISOO Directive No. 1. More than half of the agencies we reviewed were not able to

document that they were providing refresher training or failed to provide training to some of their components. Five of the agencies could not demonstrate that they administer initial briefings to new personnel and four were not providing specialized training for security managers. At a third of the agencies reviewed, some OCAs were not getting training regarding their OCA responsibilities, and at three agencies, employees who had been granted access to classified information left the service of the agency without receiving a termination briefing. These types of required training are essential to ensure that cleared personnel gain an understanding of the policies, principles, and procedures for creating, handling, and declassifying national security information.

---

### **An active self-inspection program is the most practical means of ensuring that classified information is protected properly and that basic security practices are emphasized within the work environment.**

---

Five of the agencies had inadequate self-inspection programs, and at four of these agencies no self-inspections were being conducted. Section 5.4(d)(4) of the E.O. 12958, as amended, requires agencies to establish and maintain an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product. An active self-inspection program is the most practical means of ensuring that classified information is protected properly and that basic security practices are emphasized within the work environment. Absent a self-inspection program, an agency will find it difficult to assess the effectiveness of its classified national security information program and to identify problem areas for resolution.

Three agencies did not have procedures for the reporting of security violations to a designated official or for conducting an inquiry or investigation

regarding loss, possible compromise, or unauthorized disclosure of classified information per section 2001.47(c) of the Directive. Two other agencies were not applying the violations' procedures they had established, resulting in inadequate reporting and documentation of violations and infractions.

## Document Reviews

**A**n important part of ISOO on-site reviews is an assessment of agencies' classified documents. ISOO examined classified documents during the general program reviews to evaluate the application of classification and marking requirements of E.O. 12958, as amended. We reviewed a total of 2,145 documents and found discrepancies in 1,202 documents (56 percent). There were a total of 1,993 discrepancies, resulting in an average of 1.66 discrepancies in each of the documents that contained errors and yielding an error rate of 92.9 errors per 100 documents. The most frequently occurring discrepancies were the application of improper declassification instructions (46.3 percent), a significant amount due to improper application of the X1–X8 markings, which have not been valid since the amendment to E.O. 12958 in 2003; the failure to apply either a “Classified By” or a “Derived From” line (2.4 percent); incomplete portion marking (16.5 percent); and the absence of a list of source materials on or with the official file or record copy of documents that were derived from multiple sources (3.2 percent).

## Upcoming Reviews

**I**n FY 2008 and beyond, we will continue the general program reviews, focusing on entities that we have not reviewed in recent years and agencies at which we found substantial deficiencies during previous reviews. We will continue to evaluate agency classification activity through document reviews, interviews of original and derivative classifiers, and the examination of agency security classification guides during the on-site reviews. We will also begin a review of the content, currency, and use of classification guides throughout the Executive branch. The upcoming year will also mark the start of annual assessments of agency declassification reviews, as noted in the declassification section of this report.

## NATIONAL INDUSTRIAL SECURITY PROGRAM

---

**U**nder Executive Order 12829, as amended, “National Industrial Security Program” (NISP), issued in 1993, the Director of ISOO, is “responsible for implementing and monitoring the National Industrial Security Program.” This monitoring responsibility is primarily exercised through the National Industrial Security Program Policy Advisory Committee (NISPPAC), a Federal Advisory Committee established pursuant to section 103 of E.O. 12829, as amended, and comprised of both Government and industry representatives.

The NISPPAC is responsible for recommending changes in industrial security policy through modifications to E.O. 12829, as amended, its implementing directive (32 C.F.R. 2004), and the National Industrial Security Program Operating Manual (NISPOM). The NISPPAC also advises ISOO on all matters concerning the policies of the NISP and serves as a forum to discuss policy issues. The NISPPAC meets at least twice each calendar year at the discretion of the Director of ISOO, who serves as its Chair, and the meetings are open to the public.

During FY 2007, the Director of ISOO called two meetings of the NISPPAC that included discussions on major issues such as personnel security clearance processing, position of trust suitability determinations, the implementation of Homeland Security Presidential Directive/HSPD-12, facility security clearance reciprocity, the handling of controlled unclassified information, certification/accreditation of information systems, industry access to threat data, and revisions of the NISPOM.

Under the auspices of the NISPPAC, two ad hoc working groups were formed to address NISPPAC action items. Both working groups were chaired by ISOO. The Personnel Security Clearance Ad Hoc Working Group, which included

representatives of OPM, DOD, and industry, was tasked with developing a comprehensive system of metrics, to include key data points, in order to measure the timeliness of end-to-end clearance processing for industry. The system of metrics was presented by DOD and OPM representatives to the NISPPAC and also included in a report to Congress under the Intelligence Reform and Terrorism Prevention Act concerning reduction in length of personnel security clearances.

The Office of the Designated Approval Authority (ODAA) Ad Hoc Working Group was the second NISPPAC working group established in FY 2007. Its purpose was to develop metrics for measuring the timeliness of the end-to-end certification and accreditation (C&A) for information systems to process classified national security information by industry. The objectives of the working group were to bring transparency to the process so that applicable participants understand the requirements and responsibilities necessary for the C&A of information systems, and to maximize efficiencies by leveraging industry’s and Government’s knowledge and expertise. The members of the working group include representatives from the Defense Security Service and industry. The group conducted meetings throughout the remainder of the fiscal year and will brief the NISPPAC membership on the results of its work.

Both Government and industry view the ad hoc working groups as a means to bring about transparency, gather empirical data, develop process improvements, and produce effective results for the program as a whole. The continuing work of the groups is reported at NISPPAC meetings and documented through the meeting minutes, which are available on the NISPPAC page of the ISOO website, see: [www.archives.gov/isoo/oversight-groups/nisppac](http://www.archives.gov/isoo/oversight-groups/nisppac)

# REPORT ON COST ESTIMATES FOR SECURITY CLASSIFICATION ACTIVITIES

## Background and Methodology

**A**s part of its responsibilities to oversee agency actions to ensure compliance with E.O. 12958, as amended, “Classified National Security Information,” and E.O. 12829, as amended, “National Industrial Security Program,” ISOO annually reports to the President on the estimated costs associated with the implementation of these Executive orders.

ISOO relies on the agencies to estimate the costs of the security classification system. Requiring agencies to provide exact responses to the cost collection efforts would be cost prohibitive. The collection methodology used in this report has consistently provided good indication of the trends in total cost. Nevertheless, it is important to note that absent any security classification activity, many of the expenditures reported herein would continue to be made in order to address other, overlapping security requirements.

The data for Government presented in this report 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 subcategories:

- **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, and mandatory declassification review programs authorized by Executive order, as well as declassification activities required by statute.
- **Information Systems Security for Classified Information:** An information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. 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 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.

## Survey Results and Interpretation

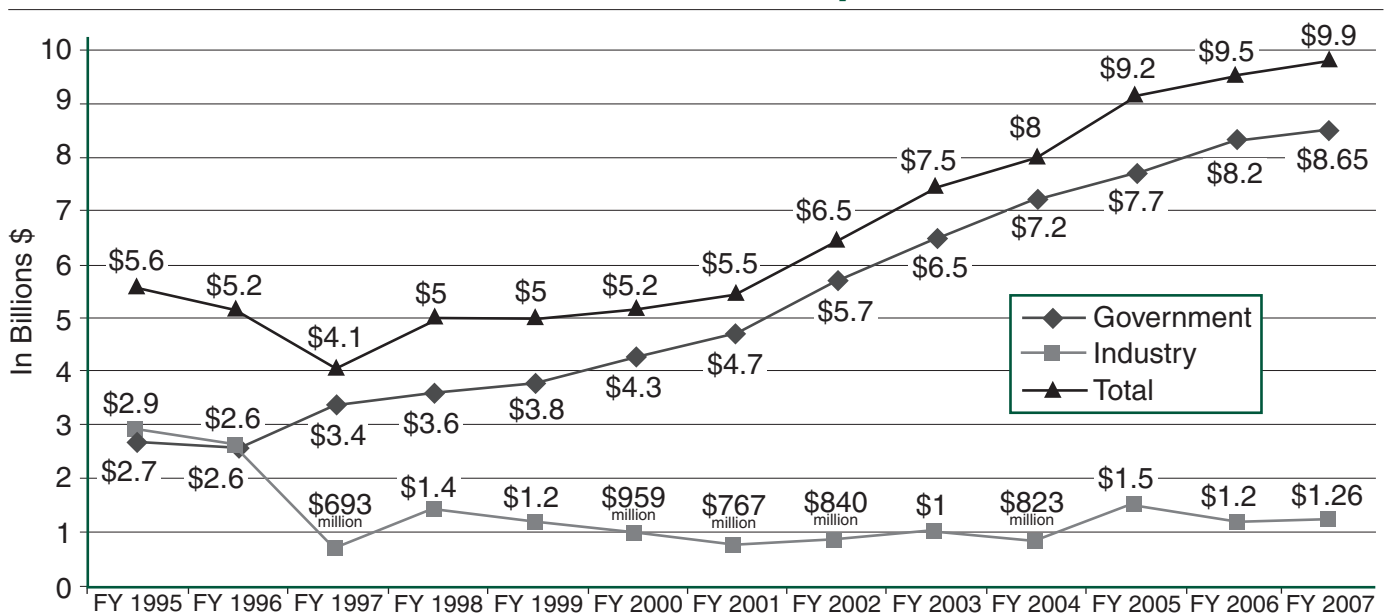
The total security classification cost estimate within Government for FY 2007 is \$8.65 billion. This figure comes from estimates

provided by 42 Executive branch agencies, including DOD. It does not include, however, the cost estimates of the CIA, NGA, DIA, the National Reconnaissance Office (NRO), and NSA, which those agencies have classified in accordance with Intelligence Community classification guidance. Those costs are however reported to ISOO.

To fulfill the cost reporting requirements of E.O. 12829, as amended, a joint DOD 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 contractor facilities. The category of facility is based on the complexity of security requirements that a particular company must meet in order to hold and perform under a classified contract with a Government agency.

The FY 2007 cost estimate totals for industry pertain to the twelve-month accounting period for the most recently completed fiscal year of each of the 593 companies that were part of the industry sample. For most of the companies included in the sample,

## Total Costs for Government and Industry for FY 1995 - FY 2007





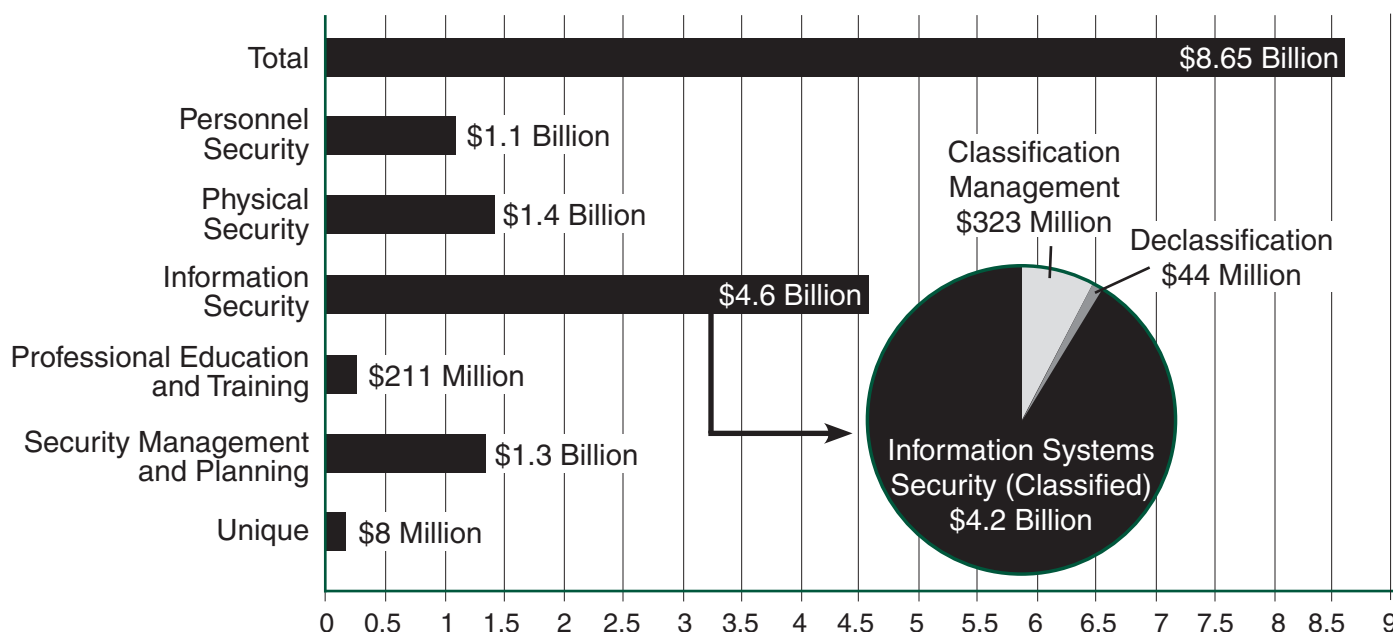
December 31, 2007, was the end of their fiscal year. The estimate of total security classification costs for FY 2007 within industry was \$1.26 billion.

As stated previously, the Government cost estimate for FY 2007 is \$8.65 billion, which is a \$415 million, or 4.8 percent increase, above the cost estimates reported for FY 2006. The industry estimate is up by \$24.6 million. This makes the total FY 2007 cost estimate for Government and industry \$9.91 billion, which is \$439 million more (4.6 percent) than the total FY 2006 cost estimate for Government and industry.

The largest increase came from the Physical Security category which experienced a \$310 million, or 22.7 percent increase. Several agencies

report that they are still developing Sensitive Compartmented Information Facilities (SCIFs), emergency operational control centers, and Continuity of Operations (COOP) sites. Some existing facilities required enhanced physical security features to bring them up to standards. Classification Management, Information Systems Security for Classified Information, and Information Security all showed an increase in FY 2007 with the cost increases in these categories, ranging from 3.3 to 3.8 percent. A decrease of 12.2 percent was reported for the Professional Education, Training, and Awareness category while the amount spent on declassification programs rose slightly (1.4 percent) after the large decrease that was reported for FY 2006.

## Government Security Classification Costs Estimate Fiscal Year 2007



## Conclusion

**A**fter an extensive surge to bolster Government-wide security measures in the post-9/11 era, the annual rate of growth for total security costs is declining. The annual rate of growth

of total security costs for FY 2006 (3.3 percent) and FY 2007 (4.6 percent) are lower than those reported for any other year since FY 2001. The average rate of growth from FY 2002 to FY 2005 was 12.11 percent, compared to an average rate of growth of 3.95 percent from FY 2006 to the present.

## AGENCY ACRONYMS AND ABBREVIATIONS

Air Force:	Department of the Air Force	Interior:	Department of the Interior
Army:	Department of the Army	ISCAP:	Interagency Security Classification Appeals Panel
CEA:	Council of Economic Advisers	ISOO:	Information Security Oversight Office
CIA:	Central Intelligence Agency	JCS:	Joint Chiefs of Staff
Commerce:	Department of Commerce	Justice:	Department of Justice
DARPA:	Defense Advanced Research Projects Agency	Labor:	Department of Labor
DCAA:	Defense Contract Audit Agency	MCC:	Millennium Challenge Corporation
DCI	Director of Central Intelligence	MDA:	Missile Defense Agency
DCIA	Director, Central Intelligence Agency	MMC:	Marine Mammal Commission
DCMA:	Defense Contract Management Agency	MSPB:	Merit Systems Protection Board
DeCA:	Defense Commissary Agency	NARA:	National Archives and Records Administration
DFAS:	Defense Finance and Accounting Service	NASA:	National Aeronautics and Space Administration
DHS:	Department of Homeland Security	Navy:	Department of the Navy
DIA:	Defense Intelligence Agency	NGA	National Geospatial-Intelligence Agency
DISA:	Defense Information Systems Agency	NISP:	National Industrial Security Program
DLA:	Defense Logistics Agency	NISPPAC:	National Industrial Security Program Policy Advisory Committee
DNI	Director of National Intelligence	NRC:	Nuclear Regulatory Commission
DOD:	Department of Defense	NRO:	National Reconnaissance Office
DOE:	Department of Energy	NSA:	National Security Agency
DOT:	Department of Transportation	NSC:	National Security Council
DSS:	Defense Security Service	NSF:	National Science Foundation
DTRA:	Defense Threat Reduction Agency	OA, EOP:	Office of Administration, Executive Office of the President
ED:	Department of Education	ODNI:	Office of the Director of National Intelligence
EPA:	Environmental Protection Agency	OIG, DOD:	Office of the Inspector General, Department of Defense
Ex-Im Bank:	Export-Import Bank of the United States	OMB:	Office of Management and Budget
FBI:	Federal Bureau of Investigation	ONDCP:	Office of National Drug Control Policy
FCC:	Federal Communications Commission	OPIC:	Overseas Private Investment Corporation
FEMA:	Federal Emergency Management Agency	OPM:	Office of Personnel Management
FMC:	Federal Maritime Commission	OSD:	Office of the Secretary of Defense
FRS:	Federal Reserve System	OSTP:	Office of Science and Technology Policy
GSA:	General Services Administration		
HHS:	Department of Health and Human Services		
HSC:	Homeland Security Council		
HUD:	Department of Housing and Urban Development		

PC:	Peace Corps	USITC:	United States International Trade Commission
PFIAB:	President's Foreign Intelligence Advisory Board	USJFCOM	United States Joint Forces Command
PIDB:	Public Interest Declassification Board	USMC:	United States Marine Corps
SBA:	Small Business Administration	USNORTHCOM:	United States Northern Command
SEC:	Securities and Exchange Commission	USPACOM:	United States Pacific Command
SSS:	Selective Service System	USPS:	United States Postal Service
State:	Department of State	USSOCOM	United States Special Operations Command
Treasury:	Department of the Treasury	USSOUTHCOM:	United States Southern Command
TVA:	Tennessee Valley Authority	USSTRATCOM:	United States Strategic Command
USAID:	United States Agency for International Development	USTR:	Office of the United States Trade Representative
USCENTCOM:	United States Central Command	USTRANSCOM:	United States Transportation Command
USDA:	United States Department of Agriculture	VA:	Department of Veterans Affairs
USD (I)	Under Secretary of Defense for Intelligence		
USEUCOM	United States European Command		





INFORMATION SECURITY  
OVERSIGHT OFFICE

---

National Archives Building  
700 Pennsylvania Avenue, NW  
Washington, DC 20408-0001

Telephone: 202.357.5250  
Fax: 202.357.5907  
E-mail: [isoo@nara.gov](mailto:isoo@nara.gov)  
Web site: [www.archives.gov/isoo](http://www.archives.gov/isoo)