Information Security Oversight Office

Report to the President

2006

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 31, 2007

The President
The White House
Washington, DC 20500

Dear Mr. President:

We are pleased to submit to you the 2006 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 review 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" (NISP).

The most significant event of the past year was the arrival of the final automatic declassification deadline of December 31, 2006, which had been a highly anticipated date since Executive Order 12958 was issued in 1995. There were times when the elimination of the existing "mountain" of classified historical records seemed impossible, and two extensions were granted in recognition of the magnitude of the task. While a detailed analysis of the final results is still underway, it appears that all Executive branch agencies have succeeded in meeting their obligations toward automatic declassification. Through the strenuous efforts of many dedicated, hard-working declassification personnel who had outstanding support from their agency's senior leadership, a task that at times appeared to be unattainable has been brought to a satisfactory culmination.

Much has been accomplished, but this good work must continue in the form of the ongoing review of the classified historical records that will become 25 years old every year. Agencies must also remember that records exempted from automatic declassification during the review process are still subject to systematic review.

The perpetual health of these declassification programs is vital to the effort to make available to the public the information that helps us understand our history, enlightens us as members of a free and democratic society, encourages relevant public discourse that may lead to more efficient governance, and informs those we elect to lead us.

Respectfully,

J. William Leonard
Director

Table of Contents

Letter to the President 1

Summary of FY 2006 Program Activity 3

State of the Executive Branch's Declassification Program 4

Declassification 6

Public Interest Declassification Board 13

Interagency Security Classification Appeals Panel 14

Classification 18

On-Site Reviews 23

National Industrial Security Program 26

Report on Cost Estimates for Security Classification Activities 28

Agency Acronyms and Abbreviations 32

Summary of Fiscal Year 2006 Program Activity

Classification

- Executive branch agencies reported 4,042 original classification authorities.
- Agencies reported 231,995 original classification decisions.
- Executive branch agencies reported 20,324,450 derivative classification decisions.
- Agencies reported 20,556,445 combined classification decisions.

Declassification

- Under Automatic and Systematic Review Declassification programs, agencies declassified 37,647,993 pages of historically valuable records.
- Agencies received 3,769 new mandatory review requests.
- Under mandatory review, agencies declassified in full 60,311 pages; declassified in part 58,883 pages; and retained classification in full on 4,275 pages.
- Agencies received 92 new mandatory review appeals.
- On appeal, agencies declassified in whole or in part 5,047 additional pages.

State of the Executive Branch Declassification Program

E.O. 12958, issued in April 1995 and amended by President Bush in March of 2003, represented a paradigm shift in the Government's declassification program. Previously, information once classified remained so indefinitely and very often did not become available to the general public, researchers, or historians without persistent and continuous effort on the part of these individuals. While all agencies had the responsibility to systematically review historical classified records for declassification, and some agencies such as the Department of State did so regularly, there was no consequence for agencies that did not conduct such reviews.

Predictably, in times of budget constraints, reviews for declassification suffered, resulting in a significant "backlog" or "mountain" of classified historical records, many of which were much older than 25 years of age. Executive Order 12958 introduced the concept of "automatic declassification," which represented consequences for agencies that did not review their historical records.

Under automatic declassification, information appraised as having permanent historical value is automatically declassified 25 years after classification, unless an agency head has determined that it falls within one of several limited exemptions that permit continued classification, subject to the approval of either the President or the Interagency Security Classification Appeals Panel (ISCAP).

After several deadline extensions, automatic declassification finally became effective on December 31, 2006, with a few notable authorized delays. As significant as the initial development of the concept of automatic declassification was, its actual implementation after so many false starts and delays is even more of an accomplishment. It reflects well on the diligence and efforts of both the public servants who accomplished this milestone through their hard work and perseverance, as well as the agencies that committed the requisite resources.

In effect, automatic declassification reverses the resource burden. Unlike previous policy, agencies had to expend resources to declassify older information. Under the current policy, agencies must expend resources to demonstrate why older historical information needs to remain classified.

Significant challenges remain. First, the Order allows a delay in automatic declassification for up to three additional years (December 31, 2009, for classified records currently 25 years old or older) that contain information of more than one agency or information the disclosure of which would affect the interests or activities of other agencies. Similarly, automatic declassification for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly may be delayed from automatic declassification for up to five additional years. Improved processes that ensure quality reviews with minimal referrals and adequate documentation regarding actual decisions made are essential.

Second, from the perspective of the public, researchers and historians, there is no "vault-full" of previously classified records that became automatically publicly available on January 1, 2007. However, in many regards, the public has already seen the major benefits of automatic declassification. Automatic declassification has served as the impetus during the recent past (since 1995) for many agencies to devote necessary resources for the establishment of substantial ongoing declassification review programs.

Since 1995, agencies have reported the

declassification of more than 1.33 billion pages of previously classified historical records. Only 257 million pages were declassified under the two previous Executive Orders governing classified information, a period encompassing almost twice as many years. Furthermore, the infrastructures established by agencies to accomplish declassification reviews since 1995 will continue indefinitely, thus contributing to the universe of declassified information as a new batch of historical records reaches 25 years of age each and every year.

WHILE SOME 460 MILLION DECLASSIFIED PAGES OF FEDERAL RECORDS HAVE BEEN MADE PUBLICLY ACCESSIBLE SINCE 1996, NARA HOLDS ANOTHER 400 MILLION PAGES OF DECLASSIFIED FEDERAL RECORDS THAT REQUIRE ADDITIONAL PROCESSING BEFORE THEY CAN BE MADE AVAILABLE.

However, declassification does not always equate to public access. Documents that have been declassified must still be reviewed to ascertain whether they contain other information that may not be releasable to the public, e.g. personal information. Also, declassified records must be accessioned and processed by archivists before they can be "put on the public shelves." These activities ensure that the National Archives and Records Administration (NARA) has both physical and intellectual control of the records. While some 460 million declassified pages of federal records have been made publicly accessible since 1996, NARA holds another 400 million pages of declassified federal records that require additional processing before they can be made available. To add to the burden, hundreds of millions of pages, both classified and recently declassified, remain within the custody of their originating agencies and will also require processing upon accession into NARA before they are made available to the public. NARA is doing its best to cope, but is woefully under-resourced to carry out its part of the process in a timely manner.

Third, a lack of resources also plagues another part of NARA, the Presidential Library system. At the Ronald Reagan Library, for example, there are over nine million pages of classified records nearing or already 25 years old, but no more than three archivists are assigned to prepare them for declassification review. There are disturbing signs that other federal agencies, having allocated the resources necessary to avoid the consequences of missing the initial December 31, 2006 deadline, now see the task as done and are contemplating cutting declassification resources. This would be a mistake. Put simply, the twin imperatives of increasing the release of formerly classified information to the public, while ensuring that information that can cause damage to national security continues to be protected, are and always will be ongoing and cannot be achieved with fewer resources.

We spend billions of dollars every year to classify information, much of which, as identified by the "9-11 Commission" and others, should never have been classified in the first place. We shortchange ourselves as a country when we do not spend the relatively paltry sums needed to declassify and make available to the public the information that helps us understand our history, enlightens us as members of a free and democratic society, encourages relevant public discourse that may lead to more efficient governance and informs those we elect to lead us.

Declassification

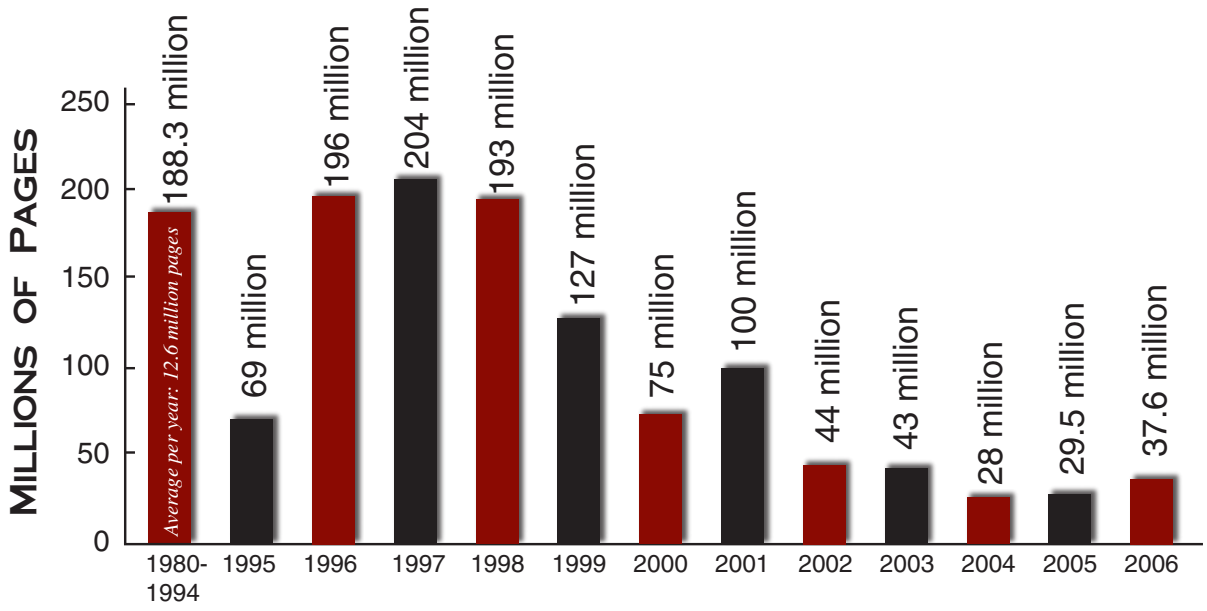
Background

E.O. 12958, as amended, establishes three pillars for the Executive branch declassification program. These are: automatic declassification, systematic declassification, and mandatory declassification review. It can not be overstated that agencies must ensure that all three of these programs required by the President continue to function at full capacity. As stated previously in this report, automatic declassification will always be with us because records will continue to reach the 25 year point every year. Systematic declassification is required to deal with classified records that are less than 25 years old and those that have been exempted from automatic declassification. Mandatory declassification review provides for direct, specific requests from the public. All three of these programs are vital to an open government and are essential to maintaining the viability of the classification system.

Pages Declassified

During FY 2006, the Executive branch declassified 37,647,993 pages of permanently valuable historical records, which is a 27 percent increase over what was reported for FY 2005. This large increase was obviously due to the final push to comply with the December 31, 2006 automatic declassification deadline. ISOO is still engaged in the process of developing a final evaluation of the Executive branch's compliance with the deadline, but we believe that by-and-large all agencies succeeded in reviewing all required materials by the deadline.

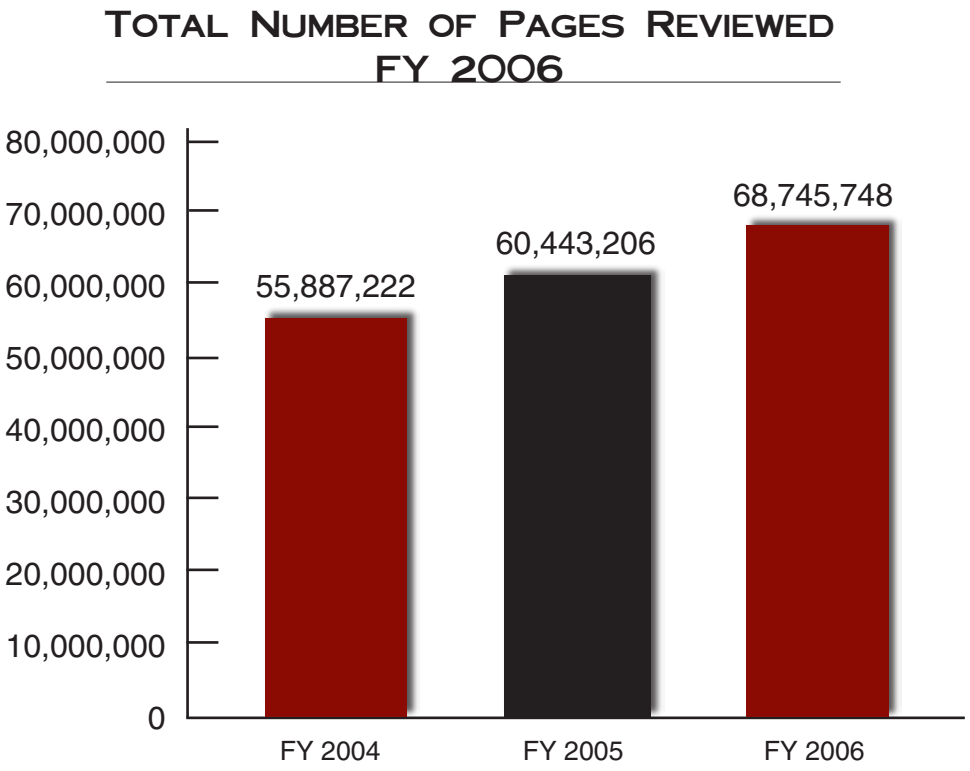
1.33 Billion Pages Declassified, FYs 1980-2006



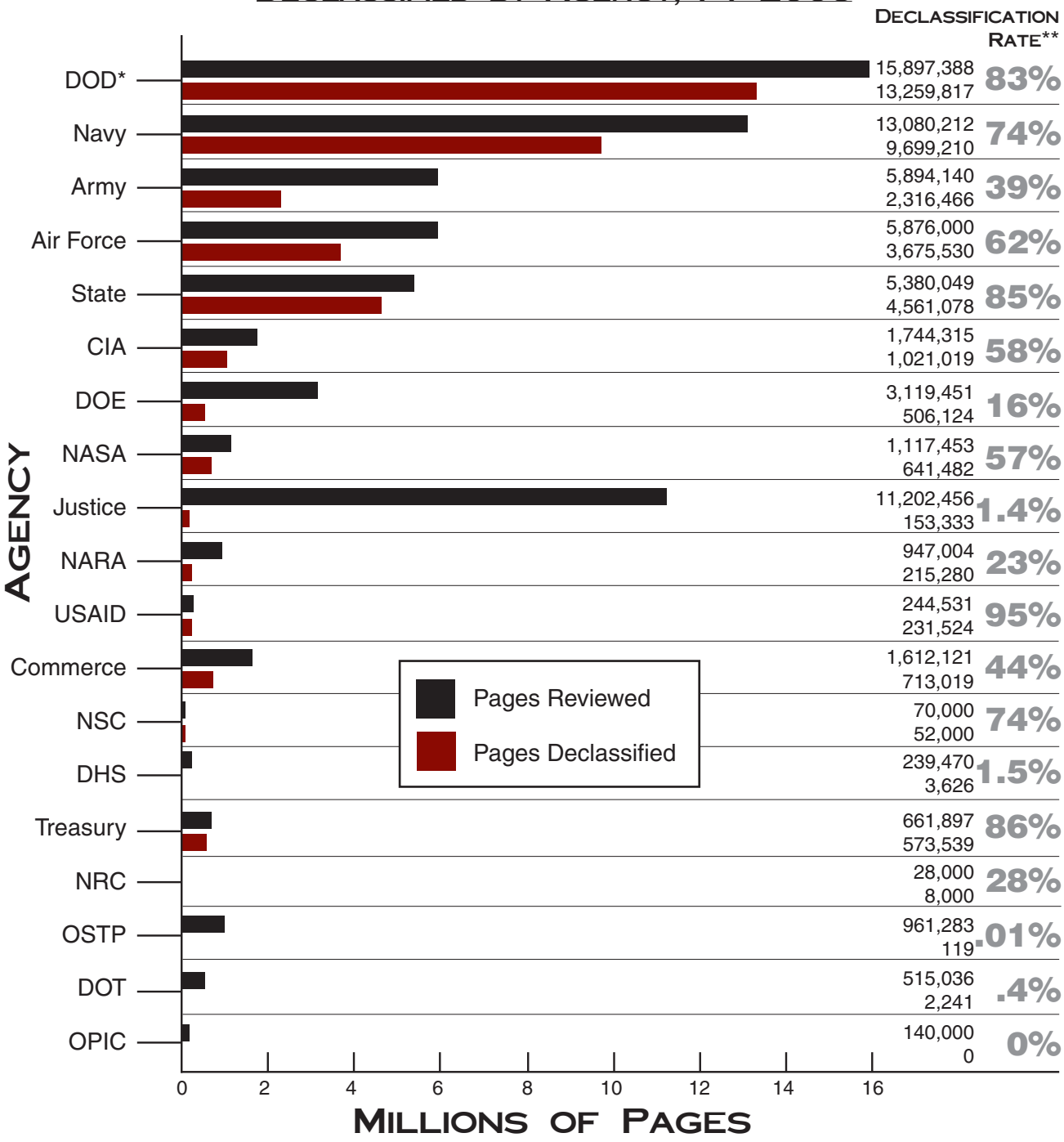
Agencies reporting significant increases in pages declassified for FY 2006 were U.S. Agency for International Development (USAID), up 141 percent, Department of Commerce (Commerce), up 813 percent, Department of Defense (DOD) up 38 percent, National Archives and Records Administration (NARA), up 38 percent, National Aeronautics and Space Administration (NASA) up 34 percent, Nuclear Regulatory Commission (NRC), up 113 percent, and Department of Treasury (Treasury), which went from 4,156 to 573,539 pages.

In FY 2004, the agencies began 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 2006 data, ISOO now has three years to compare. In FY 2004, the 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. The FY 2006 numbers reveal that agencies are now declassifying close to 55 percent of the materials they review.

In terms of the total number of pages reviewed in FY 2006, the biggest boost came from DOD and Department of Justice (Justice), which reported an increase of more than 7 million and 5 million pages, respectively. Other agencies with significant increases included the Department of Homeland Security (DHS), Department of Energy (DOE), Department of Transportation (DOT), the Overseas Private Investment Corporation (OPIC), and the Office of Science and Technology Policy (OSTP).



Number of Pages Reviewed and Declassified by Agency, FY 2006



TOTAL: 68,745,748 pages reviewed
37,647,993 pages declassified

55% 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 Executive Order 12958, as amended, the Mandatory Declassification Review (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.

A Note Regarding Agency Compliance

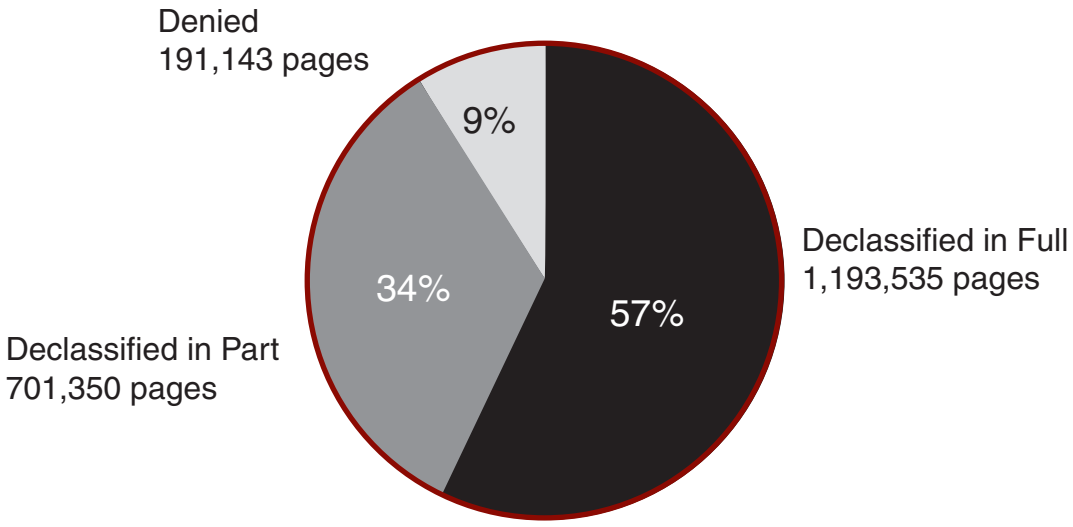
Compliance with the MDR provisions of the Order and Directive is not optional and MDR is not a "fair-weather" program. Since the issuance on December 14, 2005 of E.O. 13392, entitled, "Improving Agency Disclosure of Information," agency representatives have informally pointed to the requirements of that Order and its focus on the requirements of the Freedom of Information Act of 1974, as amended (FOIA), when speaking to their compliance with the MDR requirements. The issuance of 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 FOIA and MDR and commit the necessary resources to ensure the effective implementation of both.

Initial Requests

Agencies processed 3,769 initial requests for MDR during FY 2006. This represents an increase of 252 from FY 2005, and is only slightly below the 3,802 average number of initial requests for MDR processed annually for the period FY 1996 through FY 2005. The total number of pages processed during FY 2006 was 123,469. This represents a decrease of 27,191 as compared to FY 2005 and is significantly less than the average number of pages (180,884) processed annually for the period of FY 1996 through FY 2005.

The processing of initial requests for MDR during FY 2006 resulted in the declassification of information in 119,194 pages, or 97 percent of the pages processed. Specifically, it resulted in the declassification of 60,311 pages in full (49 percent) and 58,883 pages in part (48 percent). Three percent, or 4,275 pages, remained classified in their entirety after being reviewed. As represented in the chart on page 10, MDR remains a very successful means of declassifying information, resulting in information being declassified in 91 percent of the pages processed from FYs 1996–2006.

Disposition of Initial MDR Requests, FY 1996-2006



TOTAL: 2,086,028 pages

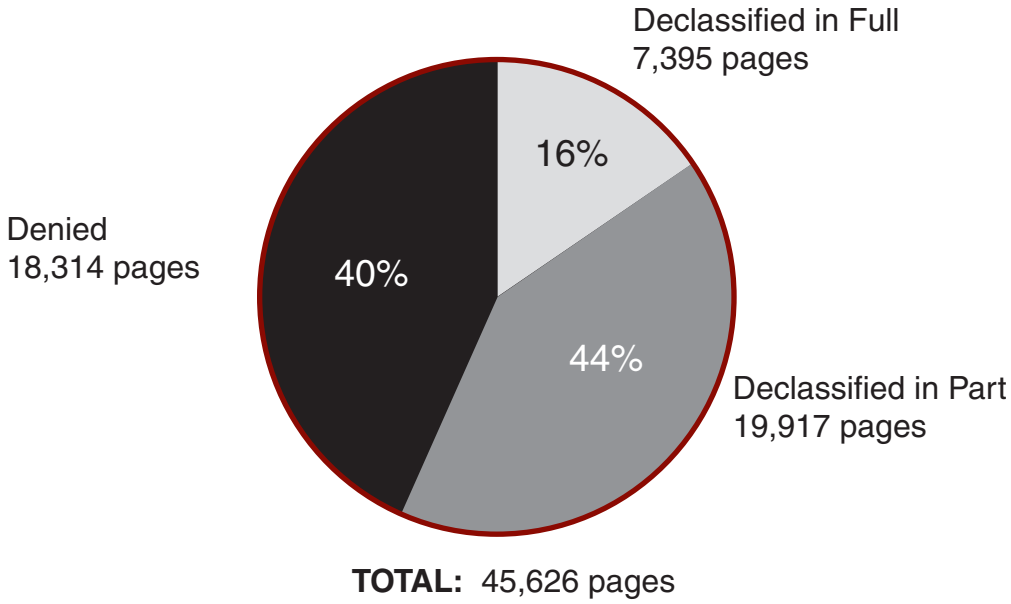
Appeals

During FY 2006, agencies processed 67 appeals of agency decisions to deny information during the processing of initial requests for MDR. This represents a significant decrease from FY 2005, when agencies processed 152 MDR appeals, and is well below the average of 106 appeals processed annually for the period FY 1996 through FY 2005. This is of particular concern as there has been no corresponding decrease in the number of new appeals received by agencies (92 in FY 2006) or in the number of old appeals carried over from FY 2005 (98 appeals). Agencies face a growing backlog of MDR appeals (123 appeal cases carried over to the next fiscal year). While NARA (78 appeals), Central Intelligence Agency (CIA) (32 appeals), and DOD (12 appeals) account for nearly all of the appeal activity, ISOO is particularly concerned about MDR appeals processing at NARA. NARA carried over 58 appeals from FY 2005 and received 26 new appeals for a total FY 2006 workload of 84 MDR appeals, but carried 78 over to FY 2007.

Agencies processed 5,558 pages as part of these MDR appeals, representing a decrease from the 8,863 pages processed in FY 2005, though slightly above the average of 4,278 pages processed annually for the period of FY 1996 through FY 2005.

The processing of MDR appeals by agencies during FY 2006 resulted in the declassification of information in 5,047, or 91 percent of the pages processed. Specifically, it resulted in the declassification of 994 pages in full (18 percent) and 4,053 pages in part (73 percent). Nine percent, or 511 pages, remained classified in their entirety after being reviewed.

Disposition of MDR Appeals FY 1996-2006



TOTAL: 45,626 pages

As the chart above illustrates, 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, 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.

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 June of 2006 ISOO hosted a MDR workshop for public and government participants that focused on the rights of a requestor and the responsibilities of government agencies. The workshop was very well received by the sixty attendees who represented both Executive branch agencies and the public. ISOO intends to provide more MDR training sessions in the future.

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**

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

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

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: **www.archives.gov/isoo/reports/2006-audit-report.html.**

As a result of this audit, the affected agencies have 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. Prior to official promulgation in regulation, this interim guidance will be fully coordinated, to include an opportunity for public comment. The interim guidance is available online at: **www.archives.gov/isoo/reports/2006-audit-report-attach-2.pdf**.

Efforts remain underway by the agencies involved, to include NARA, to restore as much of the withdrawn materials as possible. ISOO will conduct a review of this activity in September 2007 and will issue a public report on the results.

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 and could dispel perceptions that such efforts are attempts to conceal official embarrassment or to otherwise attempt to "rewrite history." To that end, ISOO has committed to report publicly on any such future actions taken after the issuance of the "Interim Guidelines Governing Re-review of Previously Declassified Records at the National Archives." ISOO intends to report on any such activity on an annual basis through its Annual Report to the President. ISOO notes that only 4 items amongst the holdings of the National Archives were withdrawn from public purview during the third and fourth quarters of FY 2006. Specifically, 2 documents (totaling 4 pages) were withdrawn at the Lyndon B. Johnson Presidential Library and 2 documents (totaling 2 pages) were withdrawn at the Jimmy Carter Presidential Library. All of these withdrawals were performed in accordance with the terms of the guidelines described above. This stands in stark contrast to the previous withdrawal activity. However, ISOO will continue to monitor such activity closely.

Public Interest Declassification Board

Introduction

In establishing the Public Interest Declassification Board (PIDB), Congress and the President 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 policy makers in the Executive branch, Congress, and the public.

Purpose

- 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.
- 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 to—
  - support the oversight and legislative functions of Congress;
  - support the policy-making 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.
- 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.
- 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.
- 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.[1]

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.

The Director of the ISOO serves as the Executive Secretary to the Board, and the ISOO staff provides support.

Additional information concerning the PIDB, including its annual report, can be found online at: **www.archives.gov/declassification/pidb/**

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

Telephone: 202.357.5250
Fax: 202.357.5907
E-mail: pidb@nara.gov

[1]Responsibility added by Section 1102 of the Intelligence Reform and Terrorism Prevention Act of 2004, which also extended the sunset clause of the Board to December 31, 2008.

Interagency Security Classification Appeals Panel

Authority

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

The Intelligence Reform Act of 2004 established the Office of the Director of National Intelligence (DNI) and amended the National Security Act of 1947 to strike the Director of Central Intelligence (DCI) from the pertinent portions. The responsibilities and the authorities of the DNI and the Director of the Central Intelligence Agency (DCIA) with regards to the ISCAP have not yet been resolved. As a result, the declassification by the ISCAP of certain information previously owned or controlled by the DCI remains pending.

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

James A. Baker
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

*The individuals named in this section were those in such positions as of the end of FY 2006.

Executive Secretary

J. William Leonard, Director
Information Security Oversight Office

Support Staff

Information Security Oversight Office

Summary of Activity

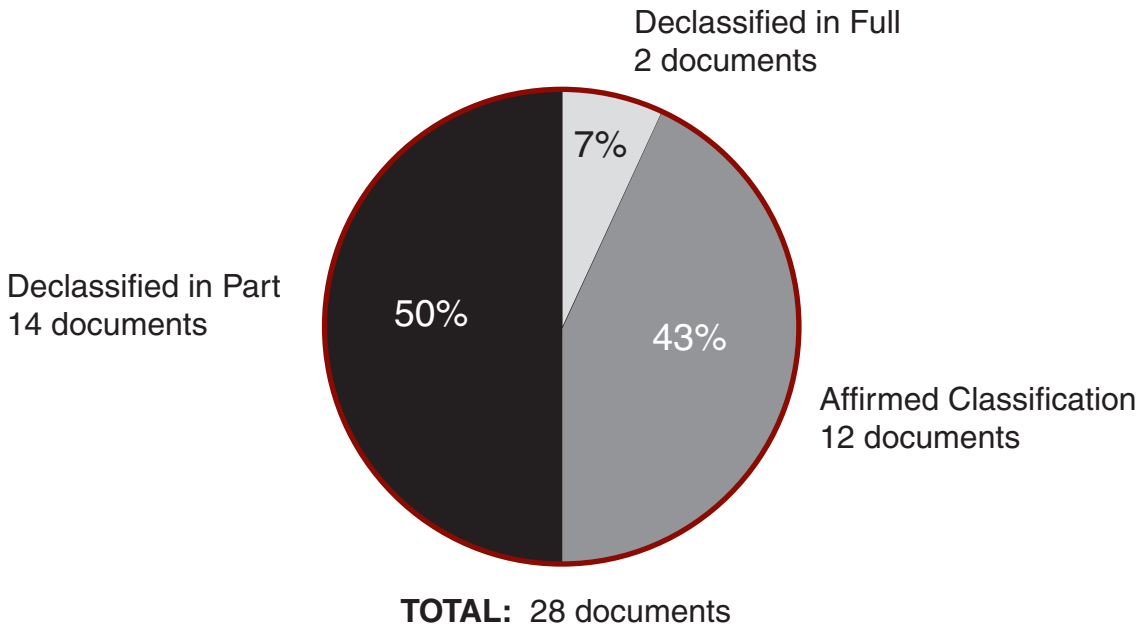
The ISCAP was created under E.O. 12958 to perform the critical functions noted above. The ISCAP, comprised of senior level representatives appointed by the Secretaries of State and Defense, the Attorney General, the DCIA, the Archivist of the United States, and the Assistant to the President for National 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. However, with the expected onset of the automatic declassification provisions of the Order on December 31, 2006, during FY 2006, the ISCAP began receiving the long-awaited influx of 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 the 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 2006, the ISCAP received 26 declassification guide submissions. This number includes new submissions, updates to previously approved guides, and instances in which agencies requested permission to utilize the approved guides of other agencies. By the end of FY 2006, the ISCAP had reviewed each submission, provided the agencies with comments and suggestions, and was awaiting revised versions to be provided by the agencies. Additionally, the submissions of the National Security Council and State were approved by the ISCAP during this time.

In addition to the review of declassification guides, during FY 2006, the ISCAP decided upon 28 documents that remained fully or partially classified upon the completion of agency processing. It declassified information in 57 percent of the documents that it decided upon, declassifying the entirety of the remaining classified information in 2 documents (7 percent) and declassifying some portions while affirming the classification of other portions in 14 of the documents (50 percent). The ISCAP fully affirmed the prior agency decisions in their entirety for 12 documents (43 percent).

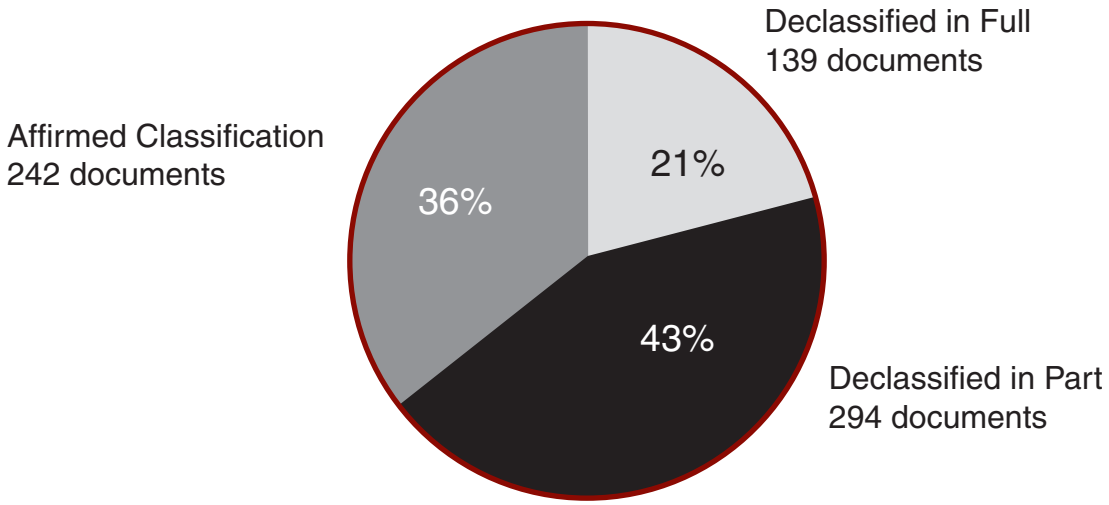
ISCAP Decisions, FY 2006



TOTAL: 28 documents

From May 1996 through September 2006, the ISCAP decided upon 675 documents. Of these, the ISCAP declassified information in 64 percent of the documents. Specifically, it has declassified the entirety of the remaining classified information in 139 documents (21 percent) and has declassified some portions while affirming the classification of other portions in 294 documents (43 percent). The ISCAP has fully affirmed agency classification decisions in 242 documents (36 percent).

ISCAP Decisions, 1996-2006



TOTAL: 675 documents

While the above chart 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 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 mentioned earlier in this report, MDRs by agencies resulted in the declassification in whole or in part, of over 97 percent of the pages reviewed. Even after such thoughtful and thorough reviews by agencies, the ISCAP declassification of additional information in 57 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.

During FY 2006, the ISCAP heard two appeals of classification challenges filed pursuant to section 1.8 of E.O. 12958, as amended. Both appeals sought to reverse the decision of the Defense Intelligence Agency (DIA) that the information within specific DIA investigative reports and briefings was classified. The information was less than 25 years

old and it concerned information related to the intelligence activities and the foreign relations of the United States. As such, the ISCAP affirmed the prior classification of both documents under sections 1.4(c) and (d) 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. 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 FYs 2004 through 2006.

However, with the amendment of E.O. 12958 in FY 2003, the 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 the amended Order).

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. As of the end of FY 2006, the second appeal remains pending and as such, the document remains classified in its entirety.

During FY 2006, neither the DNI nor the DCIA blocked the declassification of any information under section 5.3(f) of the amended Order. As noted above, the responsibilities and authorities of the DNI and the DCIA with regards to the ISCAP have not yet been resolved.

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

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

Classification

Overview

The level of reported original classification activity in FY 2006 has decreased for the second year in a row. Despite an increase of original classification activity at Justice, a reported decrease of 35 percent from DOD was the main cause of the overall decline.

Original Classifiers

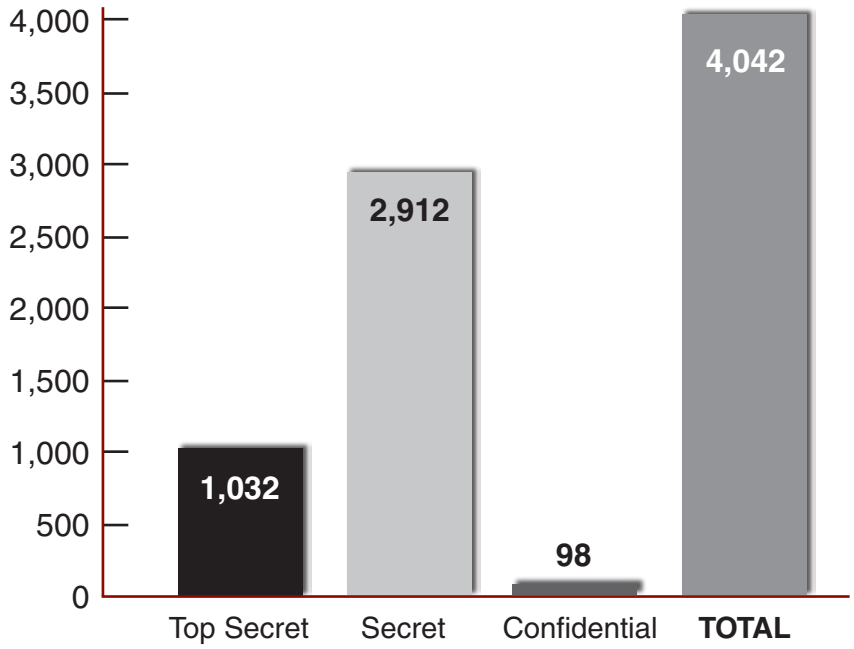
Original classification authorities (OCAs), also called original classifiers, are those individuals designated in writing, either by the President or by selected agency heads, to classify information in the first instance. Under E.O. 12958, as amended, only original classifiers determine what information, if disclosed without authority, could reasonably be expected to cause damage to the national security. Original classifiers must also be able to identify or describe the damage.

There was an increase in the number of OCAs during FY 2006 that came mainly from State and the ODNI, which is still in the formative stages of its development. The net effect was an increase from 3,959 to 4,042 or 2 percent.[2]

Original Classification

Original classification is an initial determination by an authorized classifier that information requires extraordinary

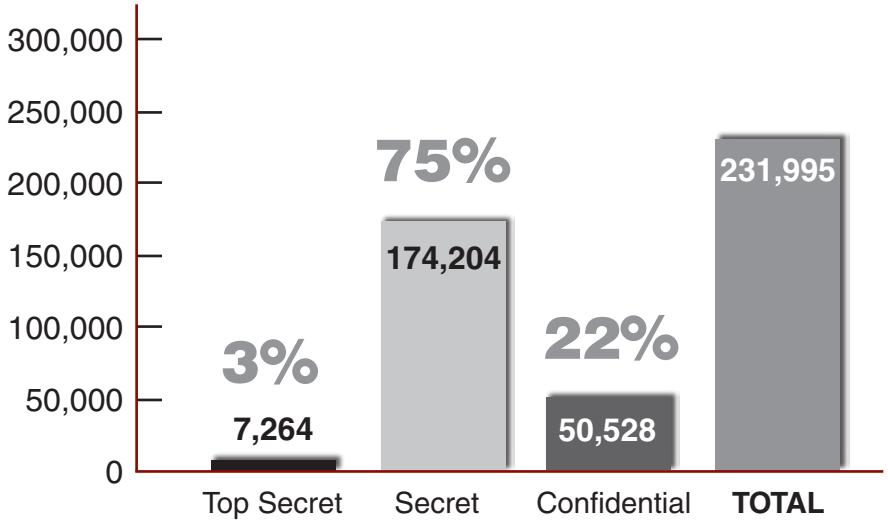
Original Classifiers, FY 2006



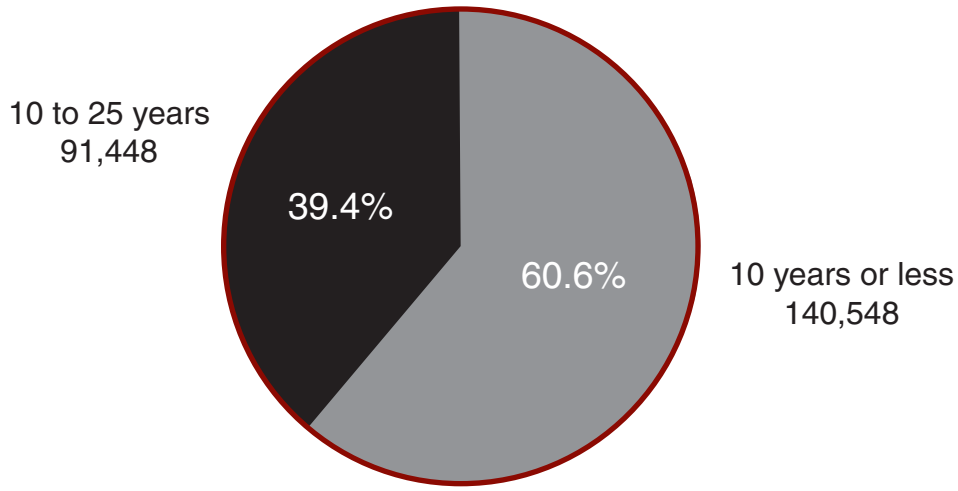
[2]The Office of the Vice President (OVP), did not report data to ISOO this year. Therefore, the reported number of OCAs does not include two OCAs previously reported by OVP. The other data reported here do not include those for OVP, which historically has not reported quantitatively significant data.

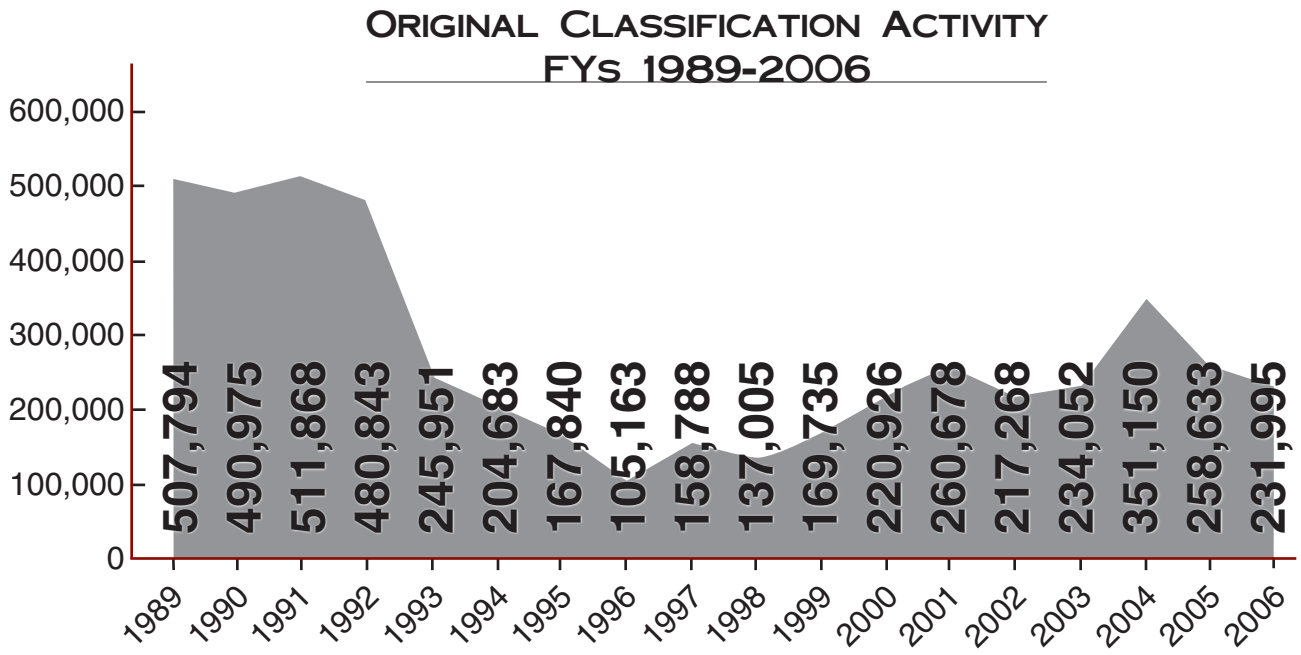
protection, because unauthorized disclosure of that information could reasonably be expected to cause damage to national security. The process of original classification always includes a determination by an OCA of the need to protect the information in the interest of national security, the placement of markings to identify the information as classified, a concise reason for the classification, 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. Simply put, it is the sole source of newly classified information.

Original Classification Activity, FY 2006



Duration of Original Classification, FY 2006





The numbers reported to ISOO for FY 2006 indicate an estimated 231,995 original classification decisions. This is 26,638 (10 percent) less than what was reported for FY 2005. The most significant decrease was reported by DOD, while Justice was up significantly. This upward movement at Justice continues to be attributed to an ongoing expansion of counterterrorism analysis at the Federal Bureau of Investigation (FBI).

For the second year in a row, the majority of original classification decisions have been assigned a declassification date of ten years or less. In FY 2006, the ten-year-or-less category came in at 61 percent, which is only slightly lower than the 64 percent reported in FY 2005. The reported results for both years represent positive change in classification practices that, we hope, will persist. Historically, under the Order, agencies selected 10 years or less 34 percent of the time in FY 2004, 52 percent of the time in FY 2003; 57 percent of the time in FY 2002; 54 percent in FY 2001; 59 percent in FY 2000; 50 percent in FY 1999; 36 percent in FY 1998; and 50 percent in FYs 1996 and 1997. This shows that original classifiers are not automatically defaulting to a 25-year declassification date, which is the maximum duration that an OCA can apply. Careful thought must be applied to every classification decision with a view to keeping the information classified only as long as absolutely necessary.

Derivative Classification

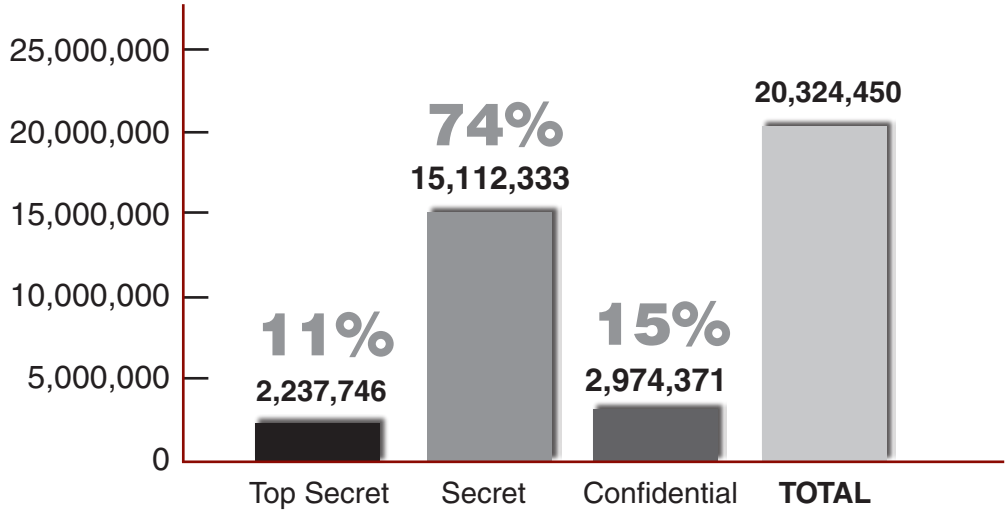
Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form classified source information. Information may be classified in two ways: (1) through the use of a source

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 identifies the elements of information about that subject that must be classified, as well as 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, and they can also replicate the same classified elements of information in a variety of formats and venues. At best, the derivative numbers provide a rough indicator of how prolific the agencies are in producing information and how much work will need to be done by declassification review teams 20 to 25 years from now. It is, therefore, important to recognize that original classification is a far more significant statistic on which to focus than derivative. For this reason, unlike previous years, we have not included a chart on combined classification activity. Also, each derivative classification decision must be able to trace its origin back to a decision by an OCA. (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 reason for overclassification.

The agencies reported a total of 20,324,450 derivative classification actions, which is a large increase over the 13,948,140 derivative actions reported in FY 2005. This increase was driven mainly by the CIA and DOD, which were up 44 percent and 58 percent, respectively. In the past, we have been able to attribute changes in the derivative data to certain external events such as the terrorist threat and operational tempo of the armed forces. This year it seems evident that the change is also attributable to efforts to improve the already massive data sampling programs that generate these derivative numbers. CIA has been refining its data sampling techniques and expanding the coverage of the sampling program. Within the last two years the office of the Under Secretary of Defense for Intelligence (USD(I)) has been taking steps to instill consistency in the sampling techniques employed throughout DOD. All consumers of this report must realize that the collection of derivative classification numbers is a challenging task for all agencies. It is noteworthy that both these agencies are working hard to improve their data collection and sampling methods.

Derivative Classification Activity FY 2006



Combined Classfication

Together, original and derivative classification decisions make up what ISOO calls combined classification activity. In FY 2006, combined reported classification activity totaled 20,556,445 decisions. The average combined classification activity since FY 2006 is 10 million actions per year. From FY 1980 through FY 1995, the FY that E.O. 12958 was issued, the annual average for combined classification was 11.5 million decisions per year.

On-Site Reviews

Summary of Activity

In FY 2006, pursuant to sections 5.2(b)(2) and (4) of E.O. 12958, as amended, ISOO conducted a total of 15 on-site reviews of Executive branch agencies. Among these were eight general program reviews of civilian and military agencies of varied sizes and seven special reviews. The general reviews evaluated the agencies' implementation of the classified national security information program to include such core elements as organization and management, classification and declassification, security education and training, self-inspections, safeguarding practices, classification markings, and security violation procedures. ISOO also conducted four special reviews of agencies' MDR programs, and three special reviews that focused on safeguarding practices and security violation handling procedures. ISOO also conducted one security assistance visit (SAV), which provided an assessment of an agency's program that was less formal than a program review. The results of the SAV are not included in this report.

General Program Reviews

The ISOO program reviews found that few of the eight agencies have adequately implemented the majority of the core elements of the classified national security information program. Shortcomings were observed at multiple agencies in their implementing regulations, self-inspection programs, document markings, and refresher security education and training. It is disappointing that these same shortcomings were noted in the ISOO FY 2004 and 2005 Annual Reports. At several agencies, the ISOO on-site review revealed inadequate support from senior management for the information security program. Sections 5.4 (a) and (b) require agency heads and senior management of agencies that originate or handle classified information to demonstrate commitment and consign necessary resources to the effective implementation of the Order.

An area of significant concern was the failure of agencies to update their regulations that implement E.O. 12958, as amended. Six agencies had not implemented revised regulations, even though the Order was amended in 2003. Implementing regulations are essential to the program because they are the foundation for agency personnel in terms of obtaining guidance and procedures pertinent to their individual responsibilities under the Order and ISOO Directive No. 1.

As found in FYs 2004 and 2005, agencies have not established comprehensive self-inspection programs. Three agencies had no self-inspection programs, and five agencies' self-inspection programs did not include a periodic review of their classified product, as required by section 5.4(d)(4) of the Order. The primary reasons for the shortcomings of these agencies' self-inspection programs were inadequate staffing levels necessary to meet their internal oversight responsibilities and insufficient senior agency official emphasis.

Self-inspections are an important element of the information security program because they enable the agency to evaluate, as a whole, its implementation of the Order's program and make adjustments and corrective actions, as appropriate.

Refresher security education and training, although an annual requirement of the Order, was not being provided at three of the agencies reviewed. This training is fundamental to the continuous reinforcement of the policies, principles, and procedures that clearance holders are expected to understand and implement.

In FY 2006, ISOO concentrated its compliance reviews on the appropriateness of classification decisions. ISOO focused on evaluating if agencies were correctly applying the Order's standards for originally and derivatively classifying information. Unfortunately, the reviews revealed source information could not be tracked when "multiple sources" was entered in the derived from line of the document classification block. Almost all agencies were not keeping a list of the source documents with the file or record copy as required by ISOO Directive No. 1. In addition, ISOO found a high percentage of documents with an unknown basis for classification, as these documents failed to indicate the authority or basis for classification, thereby calling into question the propriety of their classification. To make clear to the holder the basis for classification and to facilitate information sharing and automatic declassification, it is imperative that the multiple sources are listed and the basis for classification is identified when classifying national security information. Another area of concern was the failure of agencies to review and update their security classification guidance at least every five years or sooner as circumstances require. In large part due to the lack of timely revision to classification guides, agencies were still using obsolete X1-X8 declassification markings, which were eliminated by the 2003 amendment of the Order. As a consequence of this erroneous action, the status of subsequent derivative classification determinations based upon such improperly marked documents is placed in legal jeopardy.

Document Reviews

An important part of ISOO on-site reviews is an assessment of agencies' classified product. ISOO examined classified documents during the general program reviews to evaluate the application of classification and marking requirements of the Order. We reviewed a total of 2,298 documents and found discrepancies in 1,708 documents (74 percent). There were a total of 2,319 discrepancies, which is an average of 1.36 discrepancies in each of the documents that contained errors, yielding an error rate of 100 errors per 100 documents. The most frequently occurring discrepancies were the use of improper declassification instructions, the inconsistent application of portion marking, and a failure to indicate the basis for classification of the documents. Nearly 39 percent of the documents had errors with regard to the declassification instructions, the most common being the continued use of the X1 through X8 exemptions, which have been invalid since the amendment to the Order in 2003. Portion markings were inconsistently applied in over 30 percent of the documents.

Of paramount concern were those documents (11.1 percent) whose basis for classification could not be identified. An essential requirement of the Order is that an OCA is the only person that is authorized to classify information in the first instance. Thus, original classifications can only be made by an OCA, and every derivative classification decision must be able to be traced to a source document(s) or classification guide(s) that are ultimately OCA decisions. The program mandates this requirement through its provision to include a "Classified By" or "Derived From" line on every classified document. Since these documents lacked this information, we could not determine the basis for their classification, thus making the appropriateness of their classification uncertain. The consequences of this shortcoming are considerable in that any future classification decisions based on these documents will be problematic due to the uncertain classification status of the sources.

Conclusions

When an agency fails to effectively implement one or more elements of the classified national security program, it weakens its entire program because each of the elements has an essential purpose that is interdependent upon the others. Implementing regulations

For an effective program, the various program elements must work together.

set the foundation for the program and establish the agency's framework to implement the Order. Deficiencies in regulations lead to gaps in the agency's implementation of the program. Classification guides are the sources that prescribe the classification of specific information. They identify the elements of information regarding a specific subject that must be classified and establish the level and duration of classification for each element. Outdated classification guides may reproduce numerous invalid derivative classification decisions, thereby undermining the legal underpinnings of the classification system provided by the Order. It is imperative that classification guides are updated to reflect the changes of the Order, in particular, eliminating the use of the invalid X1-X8 markings.

Security education and training briefings inform/remind agency personnel of their duties and responsibilities and on the proper procedures for creating, handling, and destroying classified information. Inadequately trained personnel are more prone to mistakes while working with classified information. Self-inspections enable an agency to evaluate the implementation of its program on a regular basis, identify areas of concern, and take corrective action, as applicable. The absence of a self-inspection program can leave problems unidentified and uncorrected and eventually put national security information at risk.

For an effective program, the various program elements must work together. An example of the interdependence of these elements can be seen in the marking of classified documents. Agency implementing regulations must reflect the marking requirements of the current Order. An up-to-date classification guide ensures proper classification and can prevent the erroneous chain reaction that otherwise would likely occur when implementing derivative classification actions. Agency personnel must be properly trained on the classification and marking of documents. Agency self-inspections that include a review of the classified product will identify marking discrepancies, should they exist. The high error rate in the documents that ISOO reviewed can only be addressed by a multifaceted effort that includes a review and update, as necessary, of implementing regulations and classification guides, a dedicated ongoing education and training effort, and regular, continuous agency oversight of the classified product.

National Industrial Security Program

In FY 2006, ISOO finalized an implementing directive to the National Industrial Security Program (NISP) Order that was promulgated in the Federal Register, 32 CFR Part 2004, as a Final Rule on April 10, 2006. The implementing directive provides additional direction to assist agencies, to include the Executive Agent and ISOO, in their implementation of the NISP.

During FY 2006, several issues continued to inhibit reciprocity in determining eligibility for access to Classified National Security Information. Statute, Executive Order, and policy explicitly require reciprocity from executive branch agencies with respect to personnel security clearances to ensure that background investigations and adjudications are conducted only when they are actually necessary. The policy also provides for timely acceptance of existing personnel security clearances from one entity, be it government, military or NISP contractor, to another.

E.O. 12968, as amended, requires executive branch agencies to accept adjudications and investigations "mutually and reciprocally" and allows for an exception only when the gaining agency has "substantial information" that might adversely affect eligibility. The "Declaration of Principles" promulgated for the NISP in FY 2004 requires reciprocity when a contractor moves from one position to another at the same or lower level of clearance. Intelligence Community Security Implementation Procedure 4-1 from 2004 requires reciprocal acceptance of eligibility determinations for contractors within the Intelligence Community. The Intelligence Reform and Terrorism Prevention Act of 2004 requires all agencies to accept each other's investigations and adjudications. It enjoins investigative and adjudicative agencies from creating additional requirements other than polygraph. During the FY 2005, E.O. 13381 (Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information) reiterated the requirement for reciprocity. In FY 2006, the Office of Management and Budget issued two memoranda for all executive departments and agencies setting forth guidance on procedures to ensure reciprocity.

Nevertheless, reports from industry under the NISP indicate that issues remain which inhibit reciprocity. Under E.O. 12829, as amended, in fulfillment of his monitoring responsibilities as Chair of the National Industrial Security Program Policy Advisory Committee (NISPPAC), the Director, ISOO, with the agreement of the NISPPAC members, undertook an initiative to track the implementation of reciprocity in industry. Data obtained through this trends survey was reported to the Office of Personnel Management (OPM).

The survey indicated that Executive branch agencies were increasingly imposing vetting requirements on contractor personnel for reasons other than accessing classified information. It also revealed a lack of recognition on the part of certain agencies, which do not frequently deal with classified information, that there is a NISP with over 750,000 contractors who have been subject to investigations and granted clearances. Consequently, ISOO formally reminded all Executive branch agencies of their responsibility to avoid needless investigations and pointed them to resources at their disposal for the verification of current clearances.

Despite uneven implementation of reciprocity, as the Chair of the Reciprocity Working Group, ISOO has championed several other initiatives to foster greater acceptance of its use. For example, under the working group's direction,

a standardized program of instruction for adjudicators was developed and promulgated for mandatory implementation executive branch wide. Other initiatives revolve around the sampling of access eligibility determinations to evaluate their adherence to the reciprocity principles, and the formulation of common definitions of essential data points for the central clearance verification system.

The NISPPAC, comprised of both Government and industry representatives, is responsible for recommending changes in industrial security policy through modifications to E.O. 12829, as amended, its implementing directives, and the National Industrial Security Program Operating Manual (NISPOM). The NISPPAC also advises ISOO on all matters concerning the policies of the NISP, including recommended changes to those policies, and serves as a forum to discuss policy issues in dispute. The NISPPAC meets at least twice each calendar year as called by the Chairman.

During FY 2006, in his capacity as Chair of the NISPPAC, the Director of ISOO called two meetings of the NISPPAC, which took place on November 15, 2005 and May 10, 2006. At both meetings, which are open to the public, discussions occurred on major issues such as personnel security clearance reciprocity, the handling of Sensitive But Unclassified information, the verification of immigrant alien employment, the effects of the Federal Information Security Management Act, position of trust suitability determinations, and revisions of the NISPOM. Presentations were made by Industry and Government representatives, including OPM and the Department of Defense. Minutes outlining the discussions and associated action items are available on the NISPPAC page of the ISOO website (**www.archives.gov/isoo/oversight-groups/nisppac**).

THE NISPPAC, COMPRISED OF BOTH GOVERNMENT AND INDUSTRY REPRESENTATIVES, IS RESPONSIBLE FOR RECOMMENDING CHANGES IN INDUSTRIAL SECURITY POLICY THROUGH MODIFICATIONS TO E.O. 12829, AS AMENDED, ITS IMPLEMENTING DIRECTIVES, AND THE NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM).

Report on Cost Estimates for Security Classification Activities

Background and Methodology

As part of its responsibilities to oversee agency actions to ensure compliance with Executive Order (E.O.) 12958, as amended, "Classified National Security Information," and E.O. 12829, as amended, "National Industrial Security Program," (NISP), ISOO annually reports to the President on the estimated costs associated with the implementation of these Orders. This marks the 12th year of reporting these costs for security classification activities to include safeguarding requirements.

In the past, the costs for the implementation of the programs to classify, safeguard, and declassify national security information were deemed non-quantifiable, intertwined with other overhead expenses. While portions of the program's costs remain ambiguous, ISOO continues to collect cost estimate data and to monitor the methodology used for its collection. Requiring agencies to provide exact responses to the cost collection efforts would be cost prohibitive. Consequently, ISOO relies on the agencies to estimate the costs of the security classification system. The collection methodology has remained stable over the past 12 years, providing a good indication of the trends in total cost. Nonetheless, 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 as follows:

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 2006 is $8.2 billion. This figure represents estimates provided by 41 executive branch agencies, including the Department of Defense. It does not include, however, the cost estimates of the Central Intelligence Agency (CIA), the National Geospatial Intelligence Agency (NGA), the Defense Intelligence Agency (DIA), the National Reconnaissance Office (NRO), and the National Security Agency (NSA), which those agencies have classified in accordance with Intelligence Community classification guidance.

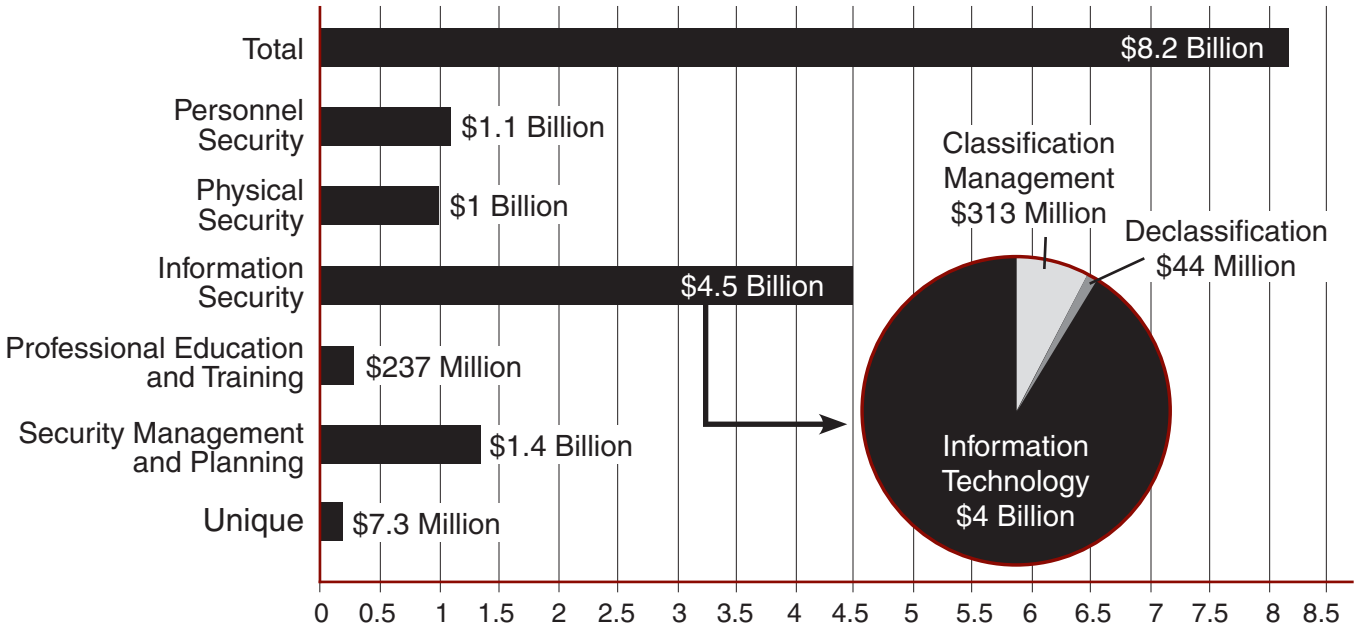
A joint Department of Defense and industry group developed a cost collection methodology for those costs associated with the use and protection of classified information within industry. Because industry accounts for its costs differently than Government, cost estimate data are not provided by category. Rather, a sampling method was applied that included volunteer companies from four different categories of 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 2006 cost estimate totals for industry pertain to the twelve-month accounting period for the most recently completed fiscal year of each company that was part of the industry sample. For most of the companies included in the sample, December 31, 2006, was the end of their fiscal year. The estimate of total security classification costs for 2006 within industry was $1.2 billion.

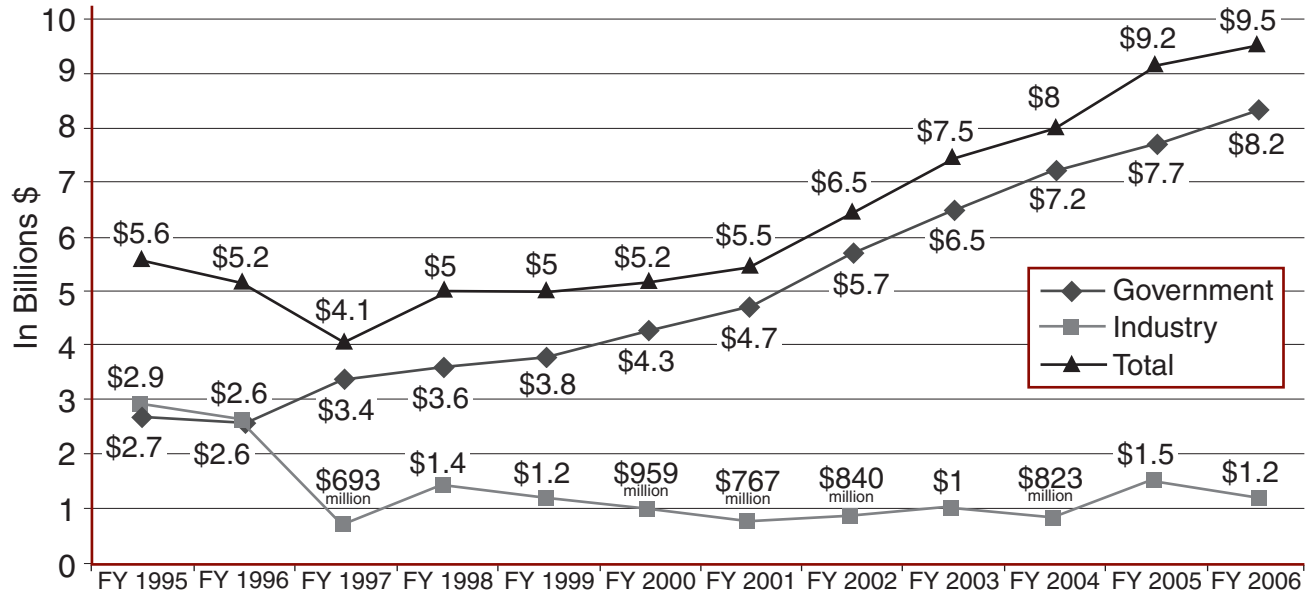
As stated previously, the Government cost estimate for FY 2006 is $8.2 billion, which is a $573 million, or 7.5 percent increase, above the cost estimates reported for FY 2005. The industry estimate is down by $263 million. This makes the total 2006 cost estimate for Government and industry $9.5 billion, which is $278 million more than the total FY 2005 cost estimate for Government and industry. This is a 3 percent increase in the Government plus industry figures, which is roughly equal to the average rate of inflation for that same time period.

The largest increase came from the Information Systems Security category, which experienced a $381 million, or 10.5 percent, increase. Many

Government Security Classification Costs Estimate Fiscal Year 2006



Graph comparing total costs for government and industry for FY 1995-2006



agencies that have never before had secure information networks are acquiring access to these networks in the interest of information sharing. In this same vein, several agencies report that they are still developing Sensitive Compartmented Information Facilities (SCIFs), emergency operational control centers, and Continuity of Operations (COOP) sites. Nevertheless, it appears that this sort of activity is leveling off since Physical Security costs only increased by 1.7 percent.

Some agencies are still reporting large increases in Personnel Security costs due to the requirement to implement the newly established standards for Personal Identity Verification (PIV) throughout the Executive branch by October 2006. Even so, the total reported expenditures in this category actually declined by 3.5 percent which suggests that the bow wave in requirements for personnel security investigations may have passed.

The reported amount spent on declassification declined by 22.6 percent even though the number of pages reviewed and the number of pages declassified actually increased. We believe this was possible because the intelligence agencies account for a very large segment of the declassification numbers and their financial data is not included in this report.

Professional Education, Training, and Awareness continued to rise in FY 2006, this time by 8.3 percent. Many agencies continue to develop state-of-the-art information security training products that are capable of reaching wide audiences, and they are also using private industry experts to assist with training management.

There was a large spike in the figures reported for the Miscellaneous (OPSEC & TSCM) category, which is due to DoD discovering TSCM resources that had previously been reported under the Information Systems Security category.

Conclusion

As noted last year, the rate of increase in the security cost estimates reported by the Executive branch agencies has apparently leveled off after the surge in security requirements and programs generated by the homeland defense concerns in the post-2001 environment. We also continue to see positive movement in categories such as training, and oversight and planning, which are important areas that ISOO frequently finds lacking during its security program reviews.

Agency Acronyms and 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
DCI	Director of Central Intelligence
DCIA	Director, Central Intelligence 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
DNI	Director of National Intelligence
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
ODNI:	Office of the Director of National Intelligence
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
USD(I)	Under Secretary of Defense for Intelligence
USEUCOM	United States European Command
USITC:	United States International Trade Commission
USJFCOM	United States Joint Forces Command
USMC:	United States Marine Corps
USNORTHCOM:	United States Northern Command
USPACOM:	United States Pacific Command
USPS:	United States Postal Service
USSOCOM	United States Special Operations Command
USSOUTHCOM:	United States Southern Command
USSTRATCOM:	United States Strategic Command
USTR:	Office of the United States Trade Representative
USTRANSCOM:	United States Transportation Command
VA:	Department of Veterans Affairs

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
Web site: **www.archives.gov/isoo**