

REPORT TO THE PRESIDENT

INFORMATION SECURITY
2011

AUTHORITY

Executive Order (E.O.) 13526, "Classified National Security Information," E.O. 12829, as amended, "National Industrial Security Program," E.O. 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," and E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." 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 Assistant to the President for National Security Affairs.

MISSION

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

FUNCTIONS

- » Develop implementing directives and instructions.
- » Review and approve agency implementing regulations.
- » Maintain liaison relationships with agency counterparts and conduct on-site and document reviews to monitor agency compliance.
- » Develop and disseminate security education materials for Government and industry; monitor security education and training programs.
- » Receive and take action on complaints, appeals, and suggestions.
- » Collect and analyze relevant statistical data and, along with other information, report them annually to the President.
- » Serve as spokesperson to Congress, the media, special interest groups, professional organizations, and the public.
- » Conduct special studies on identified or potential problem areas and develop remedial approaches for program improvement.
- » Recommend policy changes to the President through the Assistant to the President for National Security Affairs.
- » Provide program and administrative support for the Interagency Security Classification Appeals Panel (ISCAP).
- » Provide program and administrative support for the Public Interest Declassification Board (PIDB).
- » Review requests for original classification authority from agencies.
- » Chair the National Industrial Security Program Policy Advisory Committee (NISPPAC) under E.O. 12829, as amended.
- » Chair the State, Local, Tribal, and Private Sector Policy Advisory Committee under E.O. 13549.
- » Member of the Senior Information Sharing and Safeguarding Steering Committee under E.O. 13587.

GOALS

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

LETTER TO THE PRESIDENT

May 18, 2012

The President
The White House
Washington, DC 20500

Dear Mr. President:

I am pleased to submit the Information Security Oversight Office's (ISOO) Report for Fiscal Year 2011, as required by Executive Order 13526, "Classified National Security Information" (the Order).

This report provides statistics and analysis concerning key components of the system of classification and declassification, as well as coverage of ISOO's reviews of Departments' and Agencies' programs. 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."

At the request of the Office of Management and Budget, ISOO partnered with the Office of the National Counterintelligence Executive (ONCIX) to assist agencies in the review of their policies and procedures for safeguarding classified national security information against unauthorized disclosure. ISOO and ONCIX conducted three on-site evaluations in this effort, employing a team comprised of security, counterintelligence, and information assurance subject matter experts drawn from ISOO, ONCIX, and other executive branch agencies. The security component, which was primarily ISOO's responsibility, assessed key elements of the agencies' programs to safeguard classified national security information, to include program management, security education and training, self-inspections, incident reporting, inquiries and investigations, and safeguarding procedures and practices. ISOO is actively participating in the new oversight regime established pursuant to Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."

Fiscal Year 2011 also marked the launch of the first executive branch-wide Fundamental Classification Guidance Review, which the Order now requires every five years. Agencies with original classification authority began comprehensive reviews of their classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified. To assist in this effort, ISOO issued detailed guidance to all the appropriate agencies and also established timelines for interim status updates. These reviews are to be completed no later than June 27, 2012 and there will be a final report summarizing the results of each review. We believe that significant results will be obtained from this program.

Respectfully,



JOHN P. FITZPATRICK
Director

TABLE OF CONTENTS

Summary of Fiscal Year (FY) 2011 Program Activity.....	1
Classification.....	2
Declassification.....	10
Reviews	19
Interagency Security Classification Appeals Panel	22
National Industrial Security Program.....	25

SUMMARY OF FY 2011 PROGRAM ACTIVITY

Classification

- » Executive branch agencies reported 2,362 original classification authorities (OCA), down from 2,378 reported in FY 2010.
- » Agencies reported 127,072 original classification decisions.
- » Agencies reported using the ten-years-or-less declassification instruction for 70 percent of original classification decisions.
- » Executive branch agencies reported 92,064,862 derivative classification decisions; a 20 percent increase from FY 2010. This increase is expected, as it reflects revised reporting requirements intended to better capture classification activity in the electronic environment.
- » Under discretionary declassification reviews, agencies reviewed 446,202 pages, and declassified 123,193 pages.
- » A total of 52,760,524 pages were reviewed for declassification and 26,720,121 pages were declassified.
- » Agencies received 10,439 initial mandatory declassification review (MDR) requests.
- » Agencies reviewed 493,372 pages under MDR, and declassified 285,312 pages in their entirety, declassified 143,421 pages in part, and retained classification of 64,639 pages in their entirety.
- » Agencies reported carrying over 9,818 initial MDR requests into FY 2012.
- » Agencies received 283 MDR appeals and processed 229 appeals.

Declassification

- » Under automatic declassification, agencies reviewed 45,197,622 pages and declassified 23,338,707 pages of historically valuable records.
- » Under systematic declassification reviews, agencies reviewed 7,116,700 pages, and declassified 3,258,221 pages.
- » Agencies reviewed 4,405 pages on appeal, and declassified 1,298 pages in their entirety, declassified 1,937 pages in part, and retained classification of 1,170 pages in their entirety.

A Note About Future Reports:

ISOO has begun to re-evaluate the elements of information that the executive branch agencies are asked to provide for this annual report. This re-evaluation covers most aspects of the reporting process, paying particular attention to the utility and efficacy of the derivative classification count. Recognizing that this count has become considerably more complex with the growth of electronic products and data of all types within the numerous classified environments, ISOO is working with its stakeholders, inside government and out, to optimize value of this annual exercise.



CLASSIFICATION

Original Classifiers

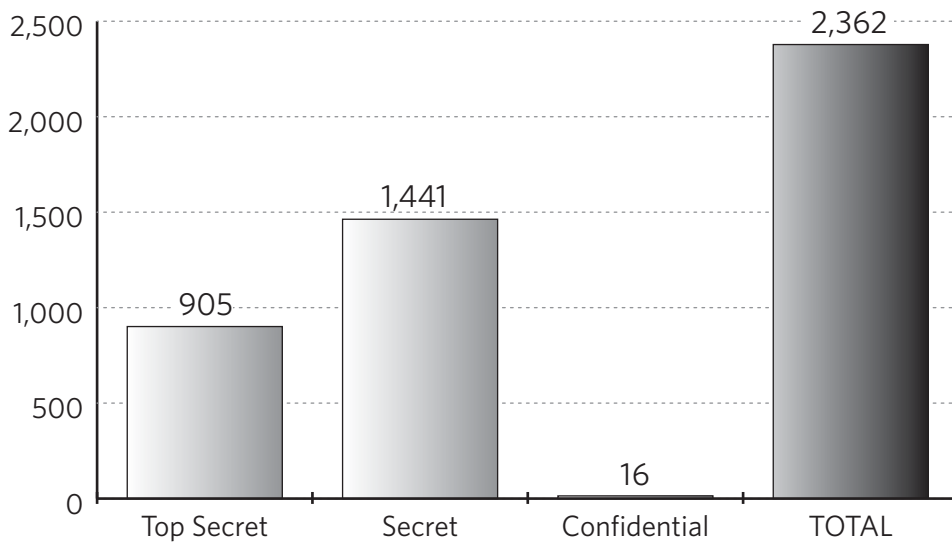
Original classification authorities, also called original classifiers, are those individuals designated in writing, either by the President, by selected agency heads, or by designated senior agency officials with Top Secret original classification authority, to classify information in the first instance.

Only original classifiers are authorized to determine what information, if disclosed without authorization, could reasonably be expected to cause damage to national security. Original classifiers must be able to identify or describe the damage.

Agencies reported 2,362 OCAs in FY 2011; a 1 percent decrease from the 2,378 reported in FY 2010.

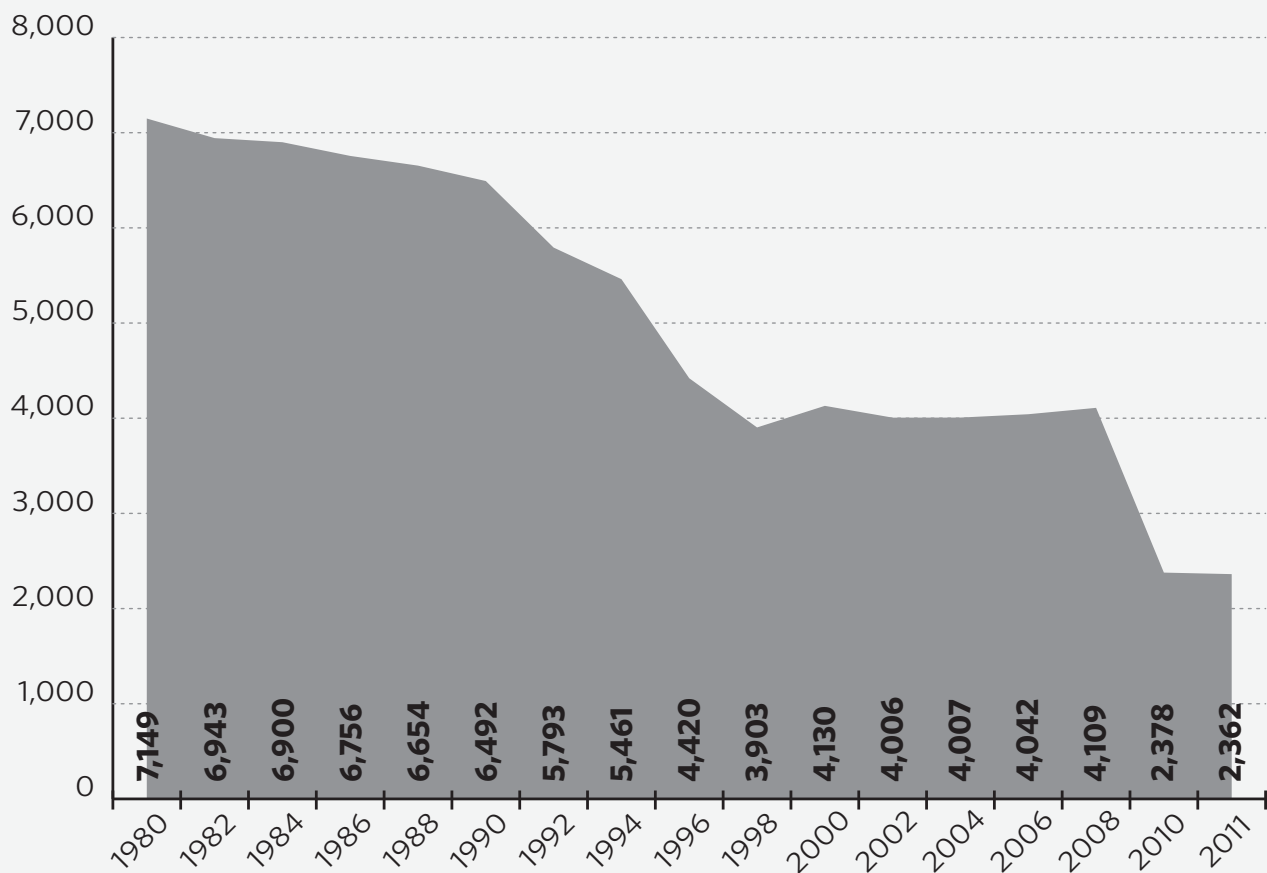
The number of original classification decisions decreased 43% from FY 2010. The primary reason for this is a greater utilization of classification guides and greater adherence to executive order guidance on the incorporation of original decisions into classification guides.

Original Classification Authorities, FY 2011





Number of Original Classification Authorities, FY 1980 - FY 2011



CLASSIFICATION

Original Classification

Original classification is an initial determination by an OCA that information owned by, produced by or for, or 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.

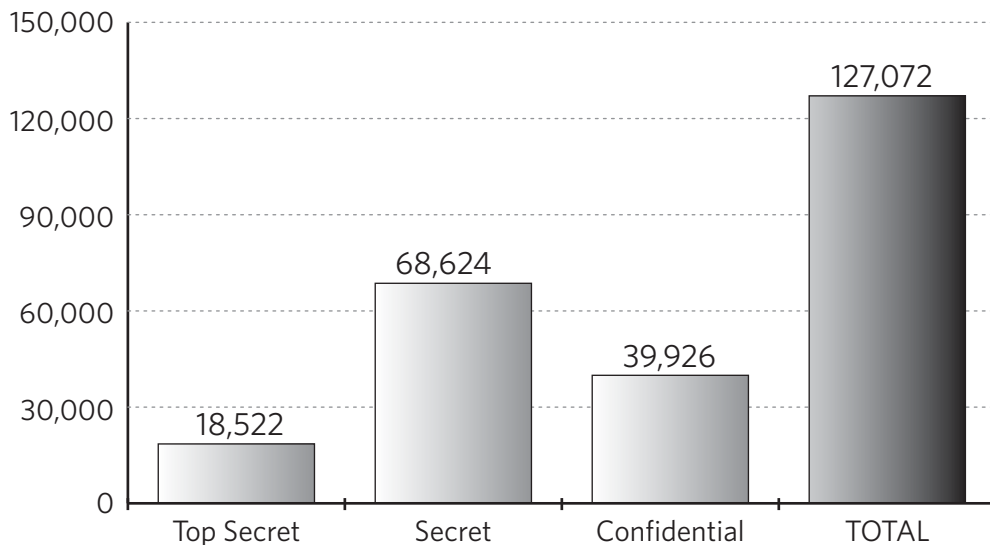
The process of original classification must always include

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.

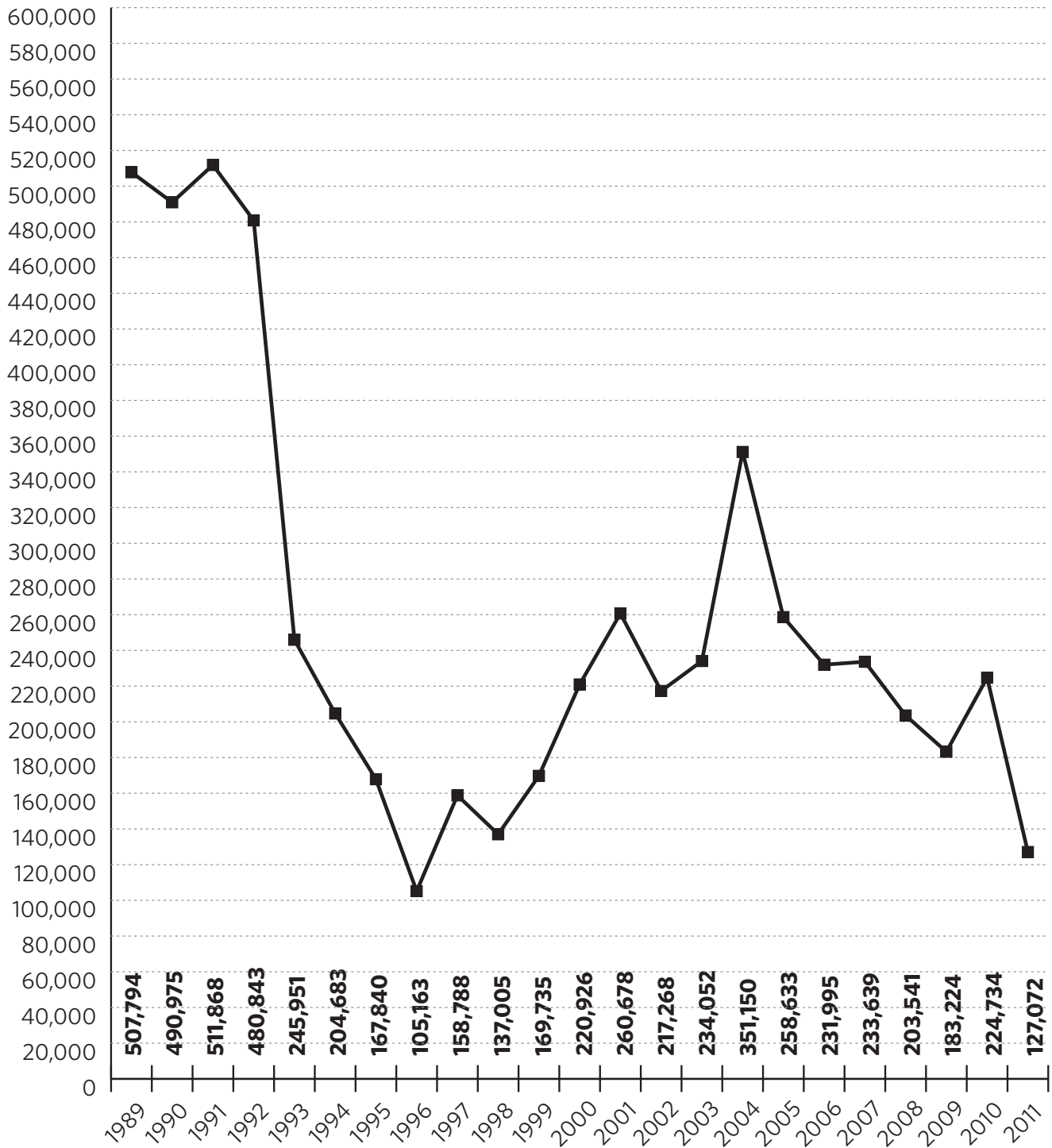
Agencies reported 127,072 original classification decisions for FY 2011 and the ten-year-or-less declassification instruction was used 70 percent of the time.

The number of original classification decisions decreased 43% from FY 2010. The primary reason for this is a greater utilization of classification guides and greater adherence to executive order guidance on the incorporation of original decisions into classification guides.

Original Classification Activity, FY 2011



Original Classification Activity, FY 1989 - FY 2011

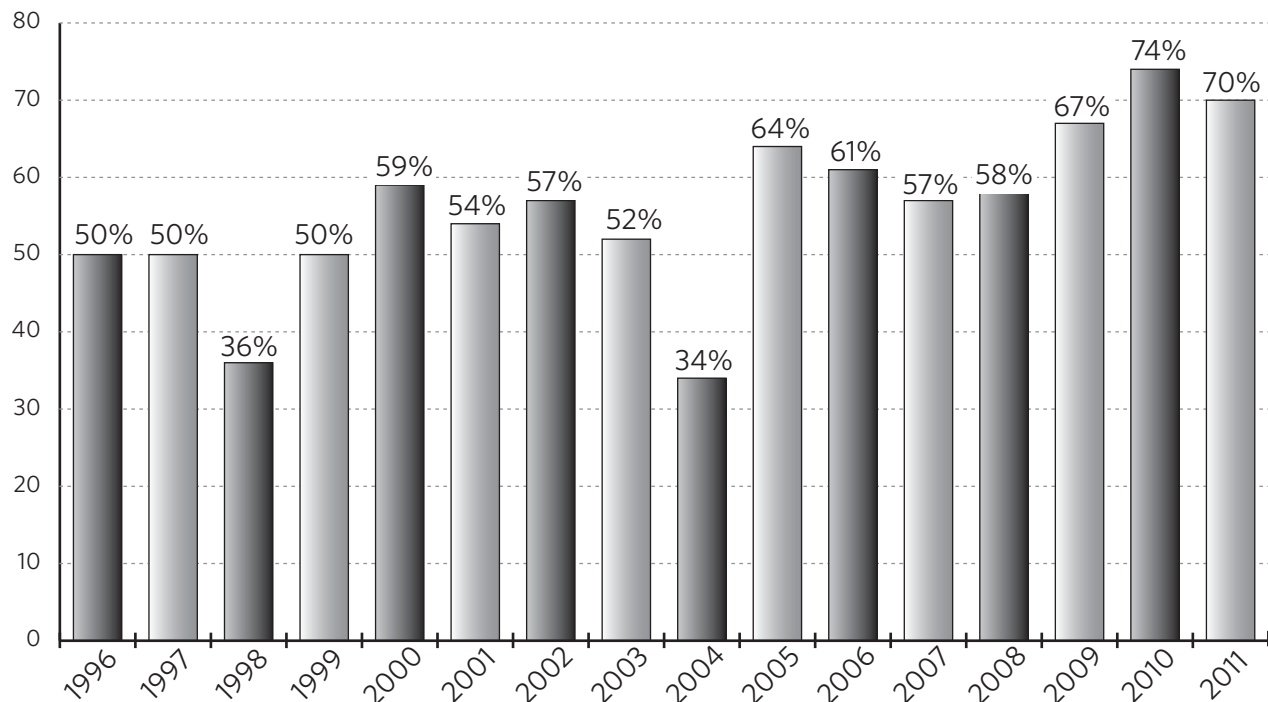


CLASSIFICATION

FY 2011 Original Classification Activity by Agency

Agency	Total Activity
Department of Defense	62,753
Department of State	48,968
Department of Justice	8,847
Department of the Army	3,468
Executive Office of the President	2,899
Department of Homeland Security	69
Department of the Air Force	42
Department of the Navy	11
Central Intelligence Agency	4
Millennium Challenge Corporation	4
Office of the Director of National Intelligence	4
Department of the Agriculture	2
Environmental Protection Agency	1
Total	127,072

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



Derivative Classification

Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified. Information may be derivatively classified in two ways: (1) through the use of a source document, usually correspondence or a publication 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 which identifies elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

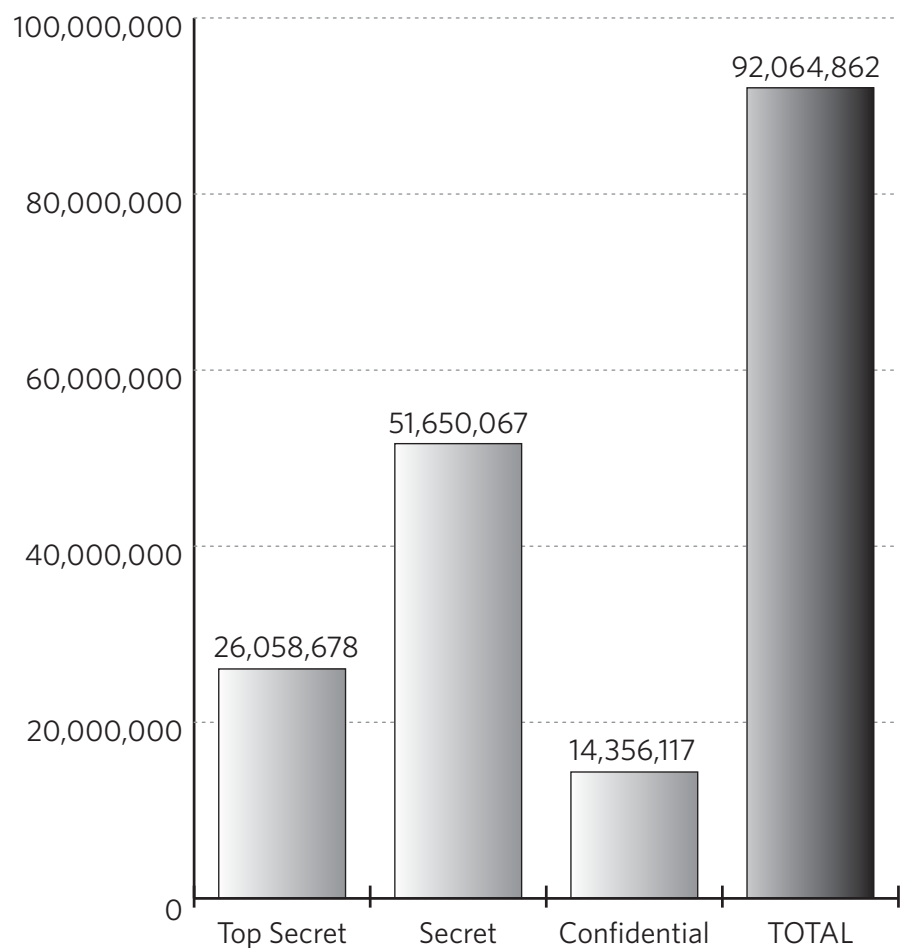
Derivative classification actions utilize information from the original category of classification. Since every derivative classification action is based on information whose classification has already been determined, it is essential that the origin of these actions be traceable to a decision by an OCA.

Agencies reported a total of 92.1 million derivative classification decisions in FY 2011. Methods for communicating classified information electronically have expanded significantly to include

classified web pages, blogs, wikis, bulletin boards, instant messaging, etc. In FY 2009, ISOO issued new guidance that asked agencies to focus on counting classification decisions in the electronic environment. This has resulted in significant annual growth in the number of derivative decisions reported. For example,

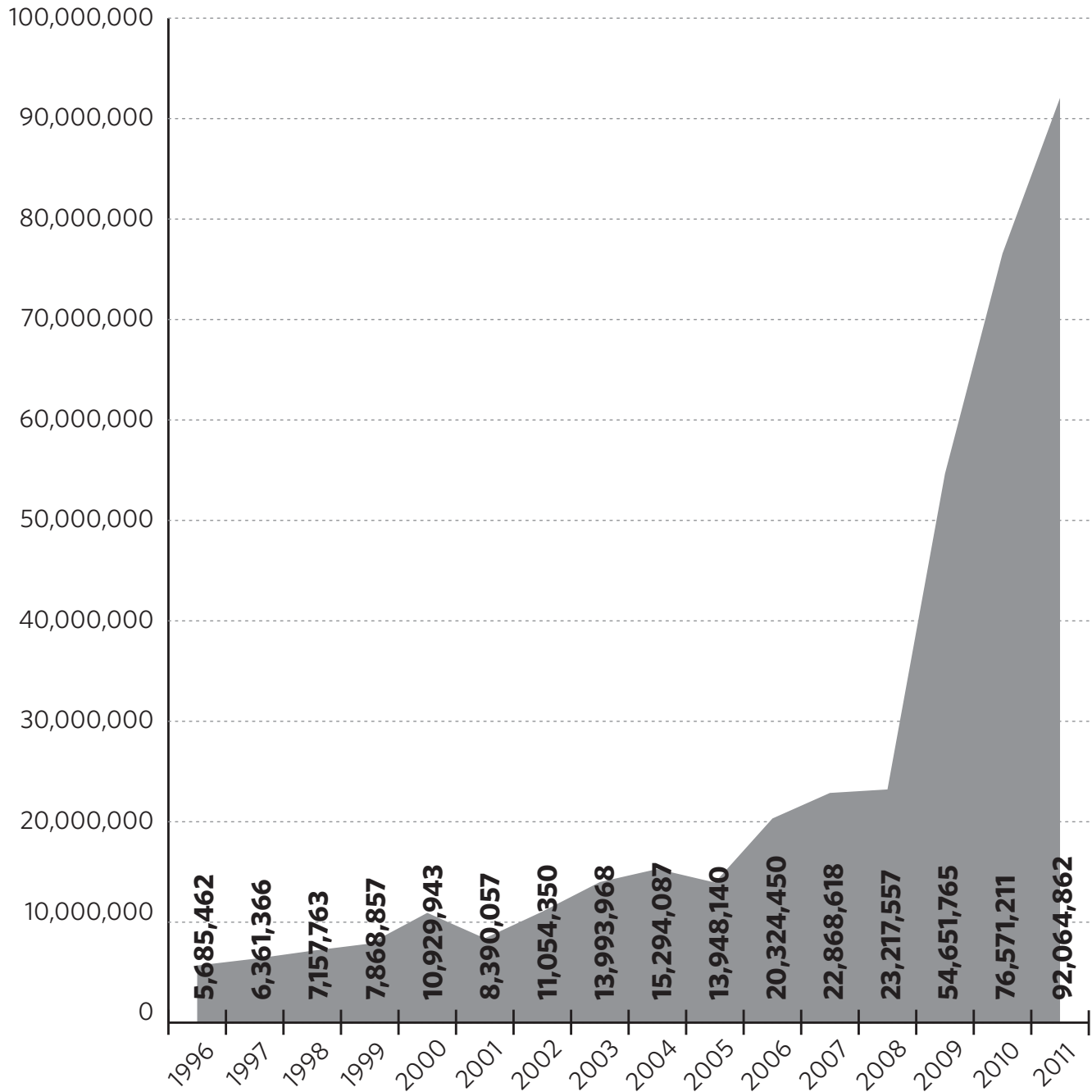
this year, the Federal Bureau of Investigation instituted a statistical sampling approach that was much more accurate than previous random sampling procedures. They were also able to capture their electronic documents count, which led to a significant increase in their number of derivative classification decisions reported.

Derivative Classification Activity, FY 2011



CLASSIFICATION

Derivative Classification Activity, FY 1996 - FY 2011



Classification Challenges

Classification challenges provide a mechanism to promote sound classification decisions. Authorized holders of information who, in good faith, believe its classification status is improper are encouraged and expected to challenge the classification status of that information. Classification challenges are handled both informally and formally, and provide individual holders the responsibility to question the appropriateness of the classification of information.

Agencies reported 79 formal challenges in FY 2011; 40 (51 percent) were fully affirmed at their current classification status with 38 (48 percent) being overturned either in whole or in part. One classification challenge remains pending.



DECLASSIFICATION

Background

Declassification is defined as the authorized change in status of information from classified to unclassified and is an integral part of the security classification system. There are four declassification programs within the executive branch: automatic declassification, systematic declassification review, discretionary declassification review, and mandatory declassification review. Automatic declassification removes the classification of information at the close of every calendar year when that information reaches the 25-year threshold. Systematic declassification review is required for those records exempted from automatic declassification. Discretionary declassification

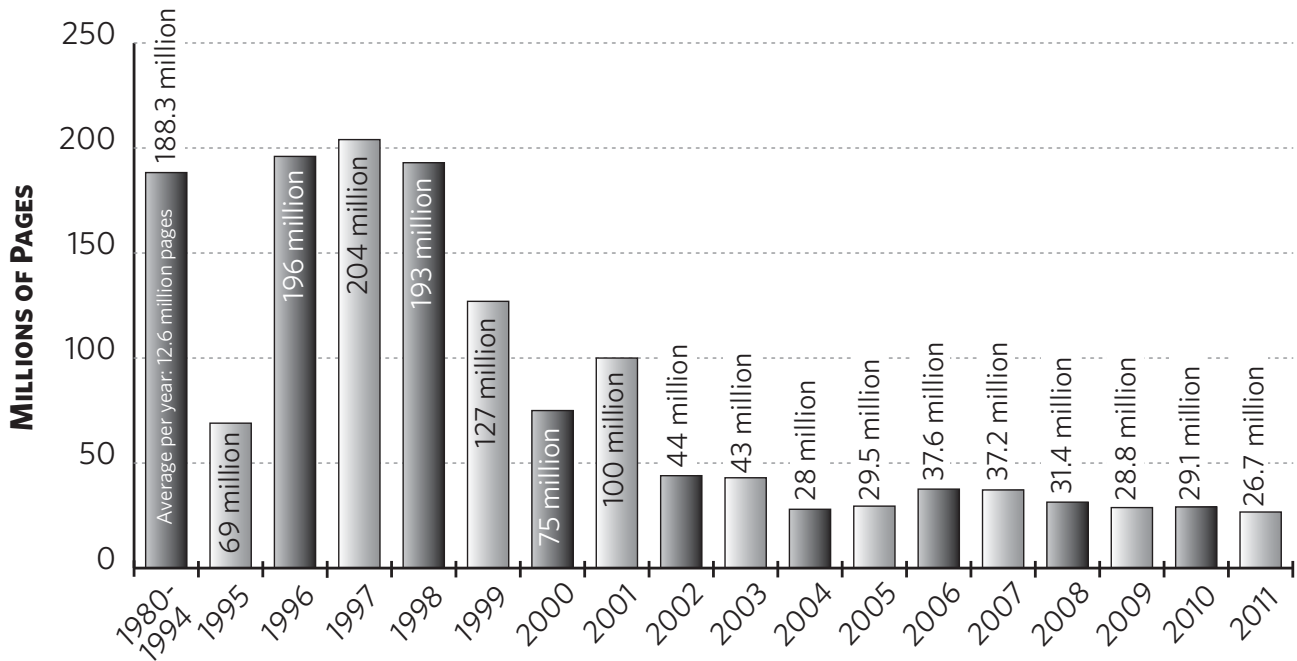
review is conducted when the public interest in disclosure outweighs the need for continued classification, or when the agency feels the information no longer requires protection and can be declassified earlier. Mandatory declassification review provides for direct, specific review for declassification of information when requested. Since 1996, statistics reported for systematic declassification review and automatic declassification were combined because the execution of both programs is usually indistinguishable. In FY 2010, however, automatic, systematic, and discretionary declassification numbers began to be reported separately. Together, these four programs are essential to the viability of the classification system and vital to an open government.

Pages Reviewed and Pages Declassified

During FY 2011, the executive branch reviewed 45.2 million pages under the automatic declassification provisions and declassified 23.3 million pages. Under systematic declassification review, agencies reviewed 7.1 million pages and declassified 3.3 million pages. Under discretionary declassification review, agencies reviewed 446,202 pages and declassified 123,193 pages. A total of 52.8 million pages were reviewed for declassification and 26.7 million pages (51 percent) were declassified.



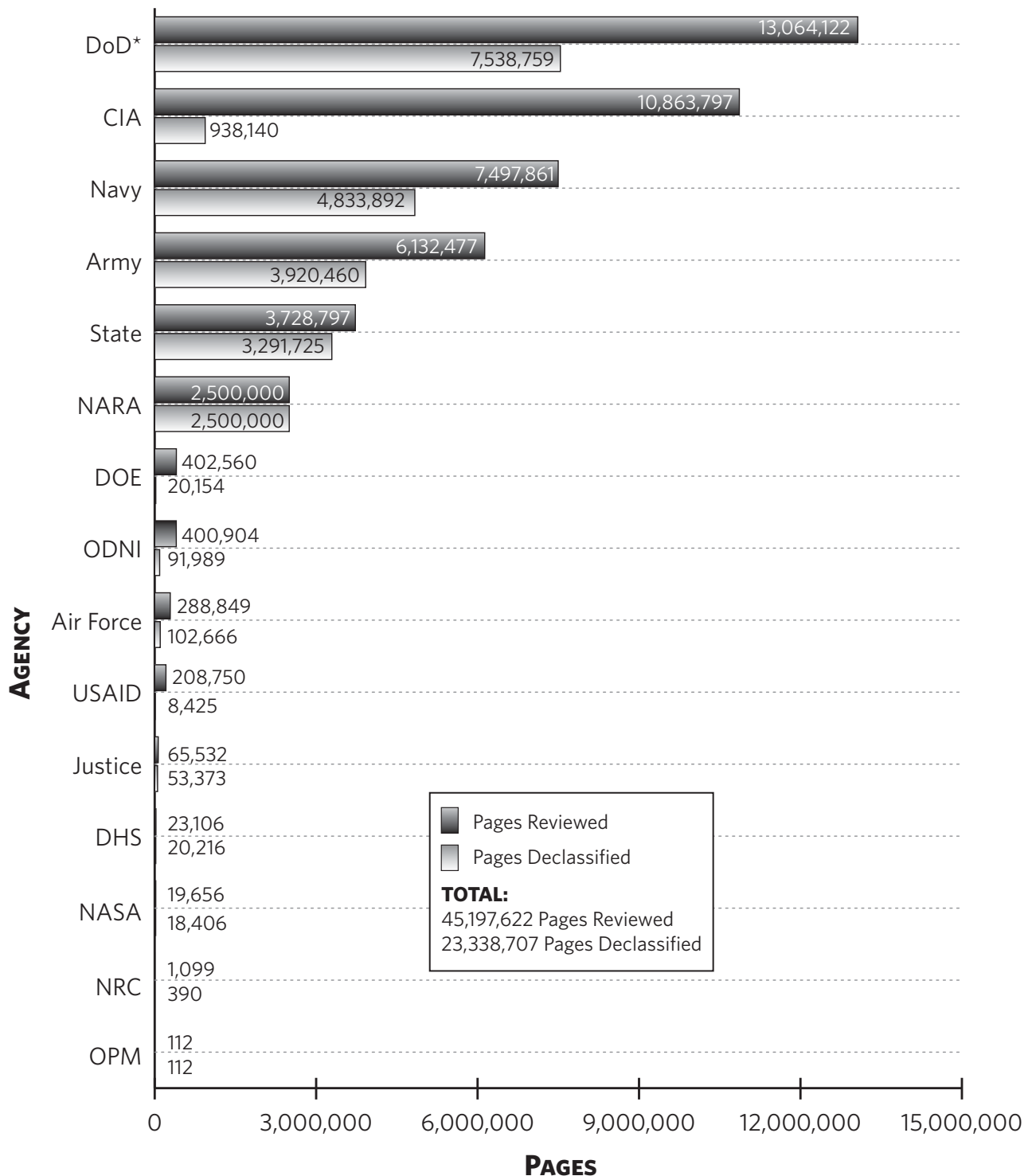
1.49 Billion Pages Declassified, FY 1980 - FY 2011*
 (Automatic, Systematic, and Discretionary Declassification Reviews)



*Excluding Mandatory Declassification Review

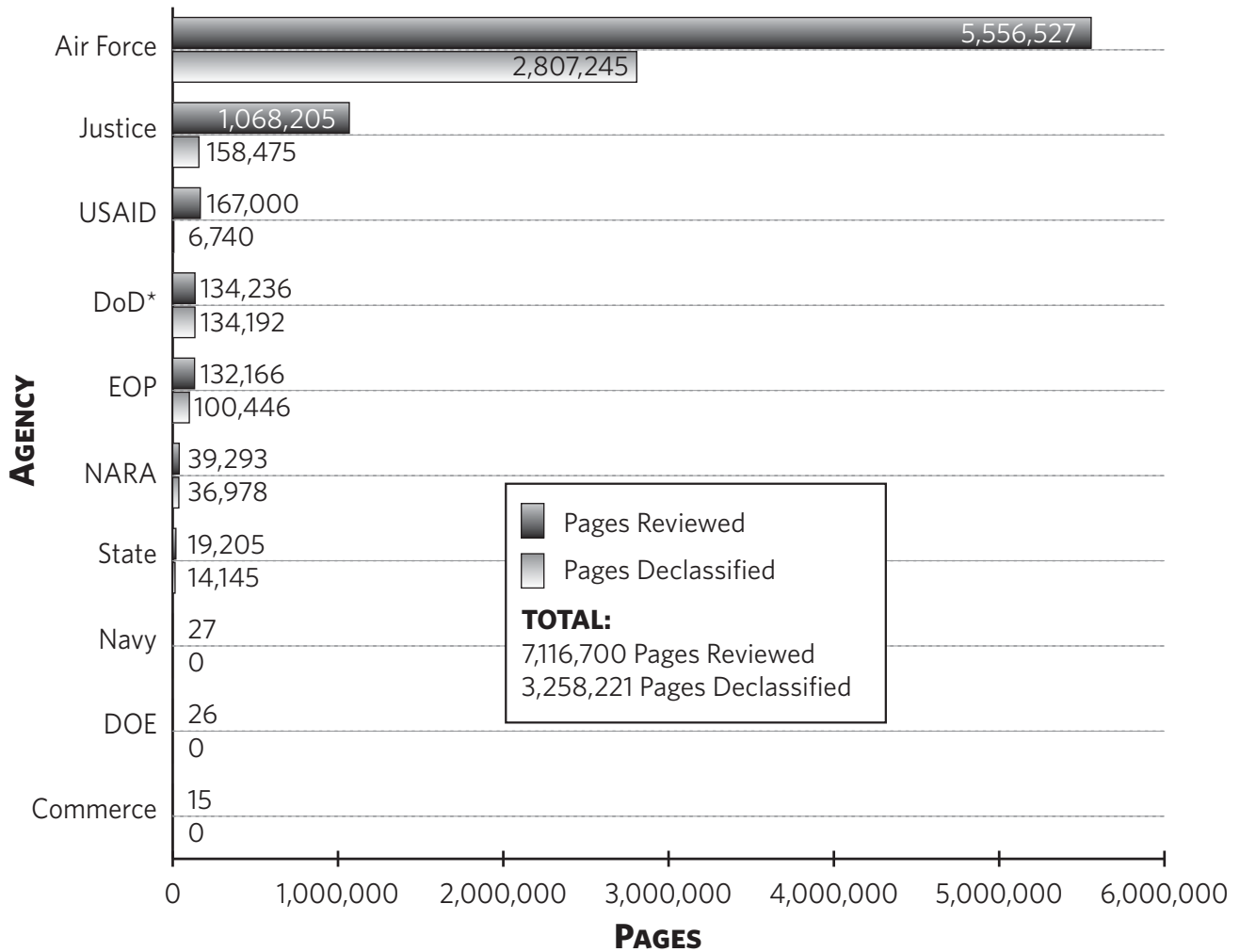
DECLASSIFICATION

Number of Pages Reviewed and Declassified for Automatic Declassification, FY 2011



*Does not include Air Force, Army, and Navy

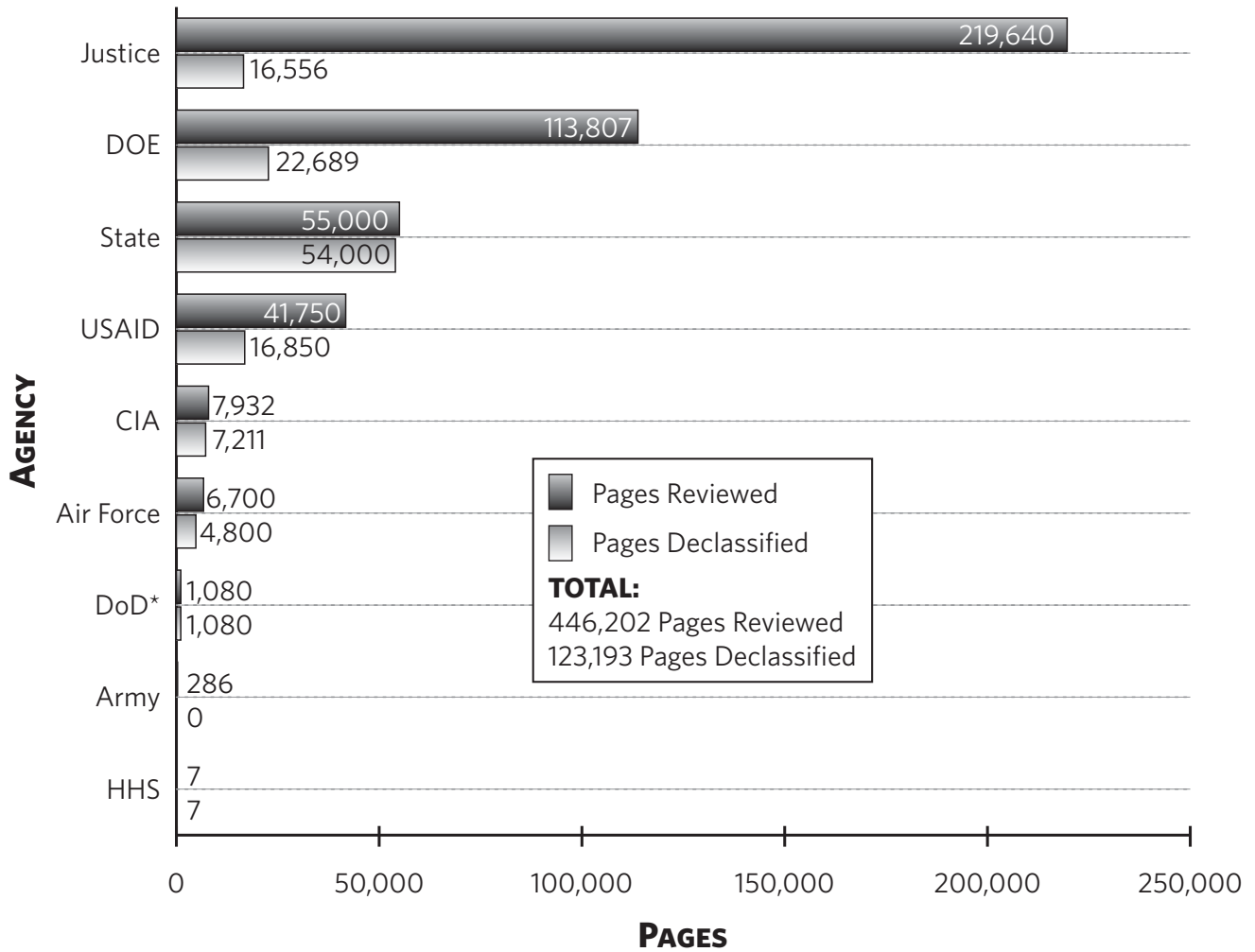
Number of Pages Reviewed and Declassified
for Systematic Declassification, FY 2011



*Does not include Air Force, Army, and Navy

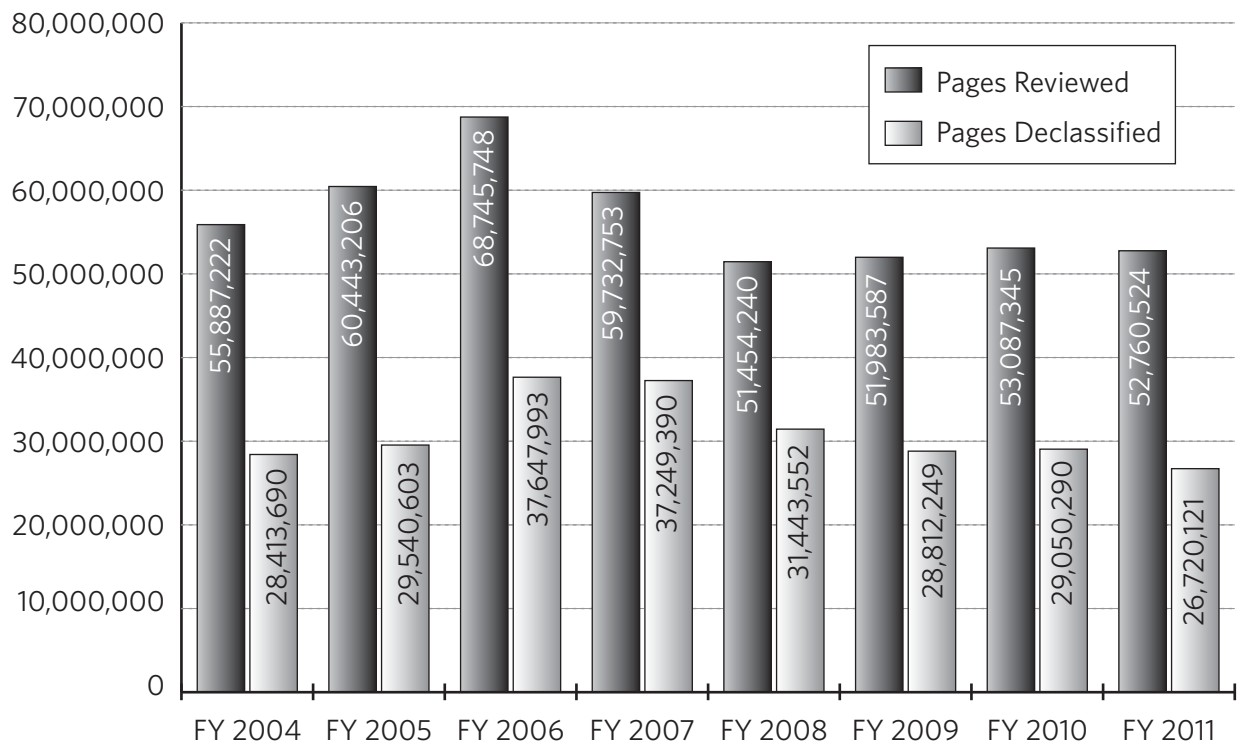
DECLASSIFICATION

Number of Pages Reviewed and Declassified
for Discretionary Declassification, FY 2011



*Does not include Air Force, Army, and Navy

Total Number of Pages Reviewed and Declassified*, FY 2004 - FY 2011
 (Automatic, Systematic, and Discretionary Declassification Reviews)



*Excluding Mandatory Declassification Review

Mandatory Declassification Review

The MDR process requires a review of specific classified national security information in response to a request seeking its

declassification. Requests must be in writing and describe the record containing the information with sufficient specificity to permit the agency receiving the request 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 (FOIA), as amended. It is also used to seek the declassification of Presidential papers or records not subject to FOIA.

DECLASSIFICATION

Initial Requests

From FY 1996 through FY 2011, agencies received an average of 5,376 initial requests per fiscal year. Agencies received 10,439 initial requests for MDR in FY 2011; 753 more than the 9,686 requests received in FY 2010. Agencies processed 10,318 requests in FY 2011, an increase of 3,592 requests from the previous fiscal year. The 10,318 requests processed in FY 2011 contained 493,372 pages. Of these, 285,312

pages were declassified in their entirety (58 percent); 143,421 pages were declassified in part (29 percent); and 64,639 pages remained classified in their entirety (13 percent).

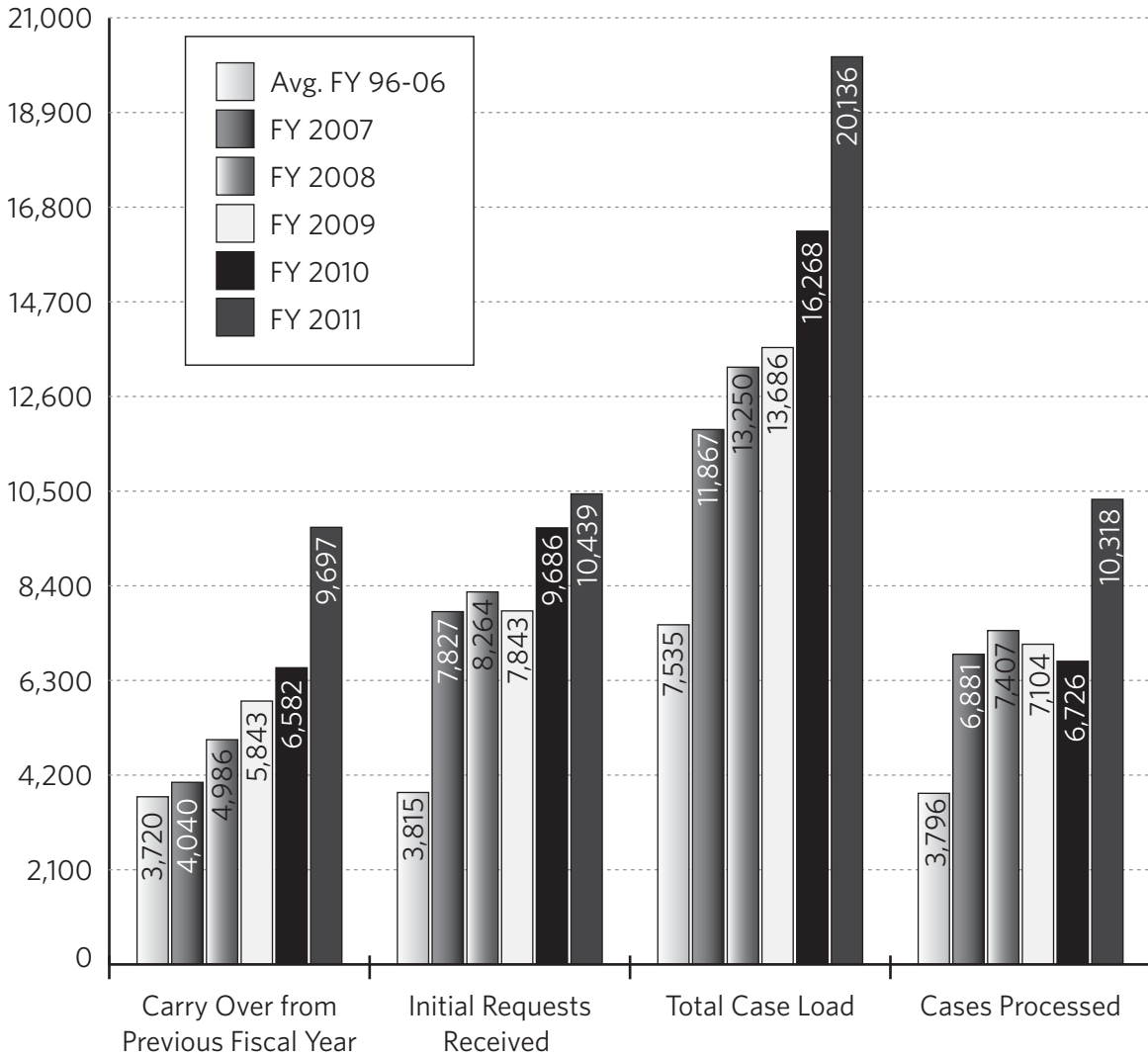
From FY 1996 through FY 2011, agencies received 86,020 initial requests and processed 3,927,477 pages. As a result of initial MDR processing, only 350,057 pages (9 percent) remained classified in their entirety after an initial MDR review: 2,433,268 pages

were declassified in their entirety (62 percent), and 1,144,152 pages were declassified in part (29 percent).

From FY 1996 through FY 2011, agencies carried over an average of 4,505 initial MDR requests from one fiscal year into the next. In FY 2010, agencies carried over 9,697 MDR requests into FY 2011, and 9,818 were carried over from FY 2011 into FY 2012.



MDR Program Activity — Initial Requests



DECLASSIFICATION

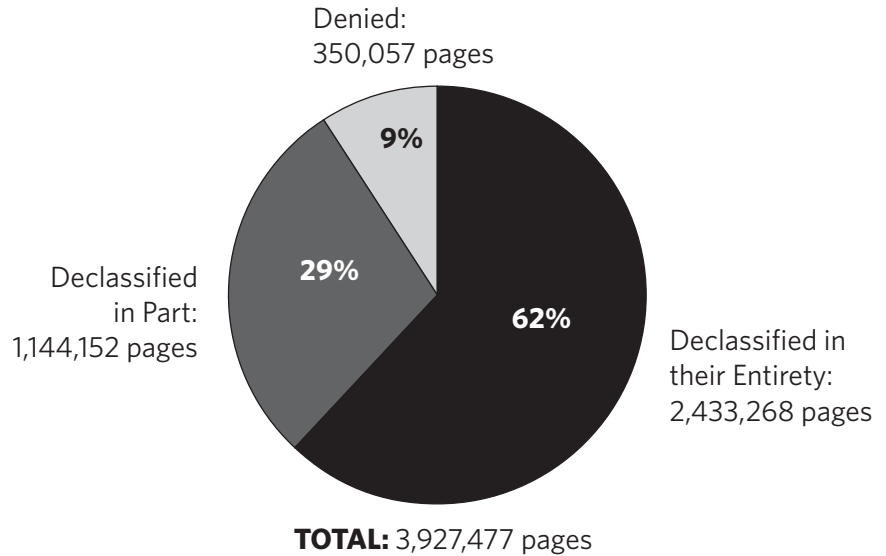
Appeals

During FY 2011, agencies received 283 appeals of agency decisions to deny information after processing and deciding upon initial MDR requests, and processed 229 appeals.

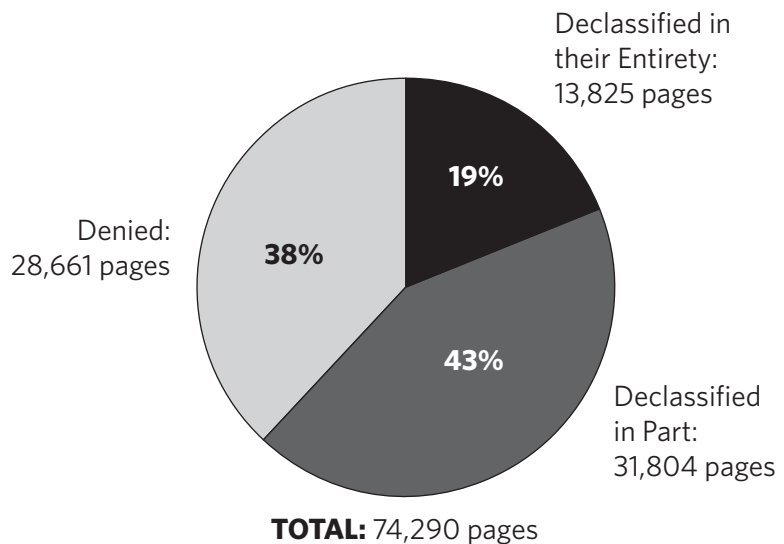
Of the appeals, agencies reviewed 4,405 pages, an increase of 1,075 from the 3,330 pages reviewed in FY 2010. The processing of MDR appeals by agencies in FY 2011 resulted in the declassification of information in 3,235 pages or 73 percent of the pages reviewed. Of these pages, 1,298 were declassified in their entirety (29 percent) and 1,937 were declassified in part (44 percent). Agencies affirmed the classification of 1,170 pages (27 percent) in their entirety.

Since FY 1996, agencies processed 74,290 appealed pages. Of these, 13,825 pages were declassified in their entirety (19 percent); 31,804 pages were declassified in part (43 percent); and 28,661 pages remained classified in their entirety (38 percent).

Disposition of MDR Requests, FY 1996 - FY 2011



Disposition of MDR Appeals, FY 1996 - FY 2011



REVIEWS

Declassification Assessments

In FY 2011, ISOO continued an initiative that began in FY 2008 to evaluate the results of agencies' automatic declassification review programs. ISOO developed this initiative as a means to evaluate agency automatic declassification review programs, disseminate the results to the agencies for the purpose of strengthening their programs, and inform the declassification community as a whole by identifying best practices and correcting common errors. Using Standard Form (SF) 311, Agency Security Classification Management Program Data, submission data from FY 2010, ISOO identified 16 agencies whose declassification programs were substantial enough to warrant assessment. Each agency was contacted in March 2011 and asked to provide information on bodies of records for which they completed declassification reviews during the six-month period from October 1, 2010, through March 31, 2011. ISOO analysts used the data collected to determine the sample size and specific documents to review during on-site declassification assessments. ISOO completed assessments of 15 of 16 agencies during FY 2011. One agency provided data that required additional research and reporting. As a result, ISOO was unable to complete the assessment of this agency in FY 2011; however, this was completed during the first quarter of FY 2012.

Assessments focused on three areas of concern: missed equities, inappropriate referrals, and improper exemptions. A missed equity indicated when the security classification interest of one agency in the record of another agency had not been identified for referral to that agency. Inappropriate referrals denoted occasions when referrals were made to agencies lacking the authority to exempt information from declassification or waiving their interest in the information. Improper exemptions included instances in which agencies attempted to exempt a record from automatic declassification under an exemption category not permitted by that agency's declassification guide as approved by ISCAP. The occurrence of any of these three issues was noted by ISOO analysts and factored into the overall agency score. In addition to these three categories of findings from within the statistical sample, ISOO analysts examined records from

outside the sample in order to develop a more complete picture of agencies' declassification programs.

Within the statistical sample, ISOO analysts encountered two examples of missed equities and only identified one instance of an inappropriate referral. ISOO did not identify any instances of improper exemptions in agency samples.

In evaluating the various programmatic aspects of agencies' automatic declassification review programs, ISOO continues to note several areas of improvement. Agencies are reviewing age-appropriate records that are between 20-25 years of age. Agencies are also appropriately using the SF 715, Declassification Review Tab, that standardizes declassification review determinations and helps facilitate the processing of referrals as well as overall archival processing. Finally, agencies are making more informed referrals. ISOO only



FY 2011 Declassification Assessment Results

Agency	Result
Central Intelligence Agency	100
Department of State	100
Federal Bureau of Investigation	100
Missile Defense Agency	100
National Archives and Records Administration	100
National Geospatial-Intelligence Agency	100
Office of the Secretary of Defense	100
Department of the Air Force	98
National Reconnaissance Office	98
Defense Intelligence Agency	94
U.S. Agency for International Development	94
Defense Threat Reduction Agency	90
Department of the Navy	90
Department of the Army	77
Joint Staff	73

identified one instance of an agency inappropriately making a referral based on letterhead instead of the content of the information.

The results of these assessments were recorded, and scores were assigned to the agencies. ISOO allocated up to 60 points for the objective findings within the statistical sample and up to 40 points for the programmatic observations, for a possible total of 100 points. Of the 15 agencies ISOO assessed, 13 received scores of 90 or above and 2 received scores from 70 to 89. No agency received a score of 69 or below. Since FY 2008, the average score

increased by over 21 percent, and the number of agencies receiving scores of 90 or above increased 125 percent.

ISOO will continue to conduct annual assessments, provide agency-specific training, and issue notices to agencies in order to provide specific guidance on areas of concern they encounter.

Fundamental Classification Guidance Review (FCGR)

ISOO issued guidance to senior agency officials outlining the requirements and providing

suggestions on how to proceed with the review process as they initiated a comprehensive review of their classification guidance. Suspense dates were established for interim status updates. Two interim reports were submitted July 29, 2011, and January 31, 2012, and provided a clear picture of agency progress. Agencies have established a comprehensive process to ensure their classification guidance is properly reviewed before the June 27, 2012, deadline. ISOO personnel have also met with numerous agency personnel to discuss specific agency progress.

Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems

During FY 2011, ISOO partnered with the Office of the National Counterintelligence Executive (ONCIX) to assist agencies in the review of their policies and procedures for safeguarding classified national security information against unauthorized disclosure. This effort was initiated in November 2010 by the Office of Management and Budget (OMB), which tasked departments and agencies to assemble teams of security, counterintelligence, and information assurance experts to perform self-assessments of their agencies' safeguarding postures. In a memorandum dated January 3, 2011, OMB informed agencies that ISOO and ONCIX would assist them in their compliance with the assessment requirement, indicating that this support would include periodic on-site evaluations where appropriate.

ISOO and ONCIX conducted three on-site evaluations, utilizing a team comprised of security, counterintelligence, and information assurance subject matter experts drawn from ISOO, ONCIX, and other executive branch agencies. The security element, which was primarily ISOO's responsibility,

assessed key elements of the agencies' programs to safeguard classified national security information, to include program management, security education and training, self-inspections, incident reporting, inquiries and investigations, and safeguarding procedures and practices.

OMB suspended these evaluations late in the fiscal year in anticipation

of the issuance of a new E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." This order was issued on October 7, 2011, and established a policy-making and oversight structure ensuring responsible sharing and safeguarding of classified information on computer networks.

E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."

INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

Authority

Section 5.3 of Executive Order 13526, "Classified National Security Information."

Functions

- (1) To decide on appeals by persons who have filed classification challenges under section 1.8 of E.O. 13526.
- (2) To approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of E.O. 13526.
- (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. 13526.
- (4) To appropriately inform senior agency officials and the public of final Interagency Security Classification Appeals Panel (the Panel) decisions on appeals under sections 1.8 and 3.5 of E.O. 13526.

Members*

William H. Leary, Chair
National Security Staff

Mark A. Bradley
Department of Justice

Margaret P. Grafeld
Department of State

Reginald D. Hyde
Department of Defense

Sheryl J. Shenberger
National Archives and
Records Administration

Corin Stone
Office of the Director of
National Intelligence

Executive Secretary

John P. Fitzpatrick, Director
Information Security
Oversight Office

Note: Section 5.3(a)(2) of E.O. 13526 provides for the appointment of a temporary representative to the Panel from the Central Intelligence Agency (CIA) to participate as a voting member in all deliberations and support activities that concern classified information originated by the CIA. That temporary representative from the CIA is Joseph W. Lambert.

Support Staff

Information Security
Oversight Office

Background

The Panel was created under Presidential executive order in 1995 to perform the functions noted above and began meeting in May 1996. The permanent membership is comprised of senior-level

representatives appointed by the Secretaries of State and Defense; the Attorney General; the Director of National Intelligence; the Archivist of the United States; and the Assistant to the President for National Security Affairs. The President selects the Chairperson, the Director of the Information Security Oversight Office serves as its Executive Secretary, and ISOO provides staff support.

Mandatory Declassification Review Appeals

During FY 2011, the Panel allocated a majority of its time and resources to processing MDR appeals. The documents within these MDR appeals came before the Panel classified either in part or in their entirety and were properly filed with the Panel in accordance with E.O. 13526 and the Panel's bylaws. In FY 2011, the Panel decided upon 51 MDR appeals, containing a total of 156 documents. The Panel declassified additional information in 92 documents (59 percent), and affirmed the prior agency classification decisions in 64 documents (41 percent). Of the 92 documents in which information was declassified, 39 documents (25 percent) were declassified in their entirety and 53 documents (34 percent) had some portions declassified while the classification of other portions was affirmed.

*Note: The individuals named in this section were in these positions as of the end of FY 2011.

Since May 1996, the Panel decided upon a total of 1,195 documents. Of these, the Panel declassified additional information in 64 percent of the documents. Specifically, 291 documents (24 percent) were declassified in their entirety and 477 documents (40 percent) had some portions declassified while the classification of other portions was affirmed. During this time frame, the Panel fully affirmed the classification decisions of agencies in 427 documents (36 percent). Documents declassified by the Panel may be requested from the executive branch agency that has custody of them. For assistance in identifying and requesting copies of such documents, please contact the Panel's support staff:

Telephone: 202.357.5250

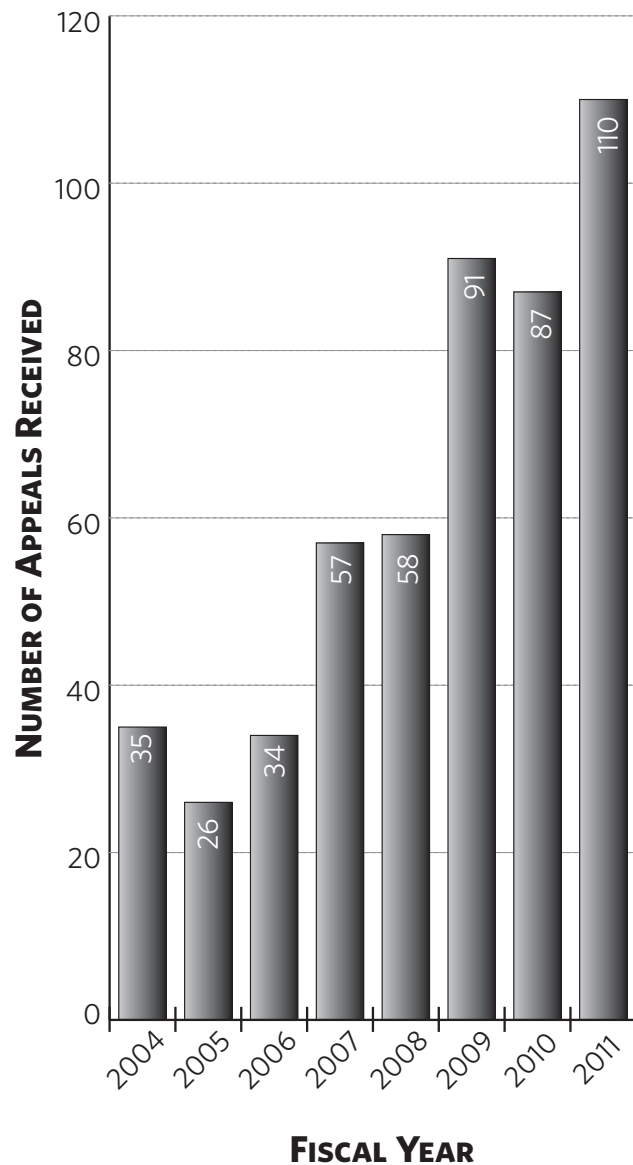
Fax: 202.357.5907

E-mail: iscap@nara.gov

Additional information may be found on the ISOO website:

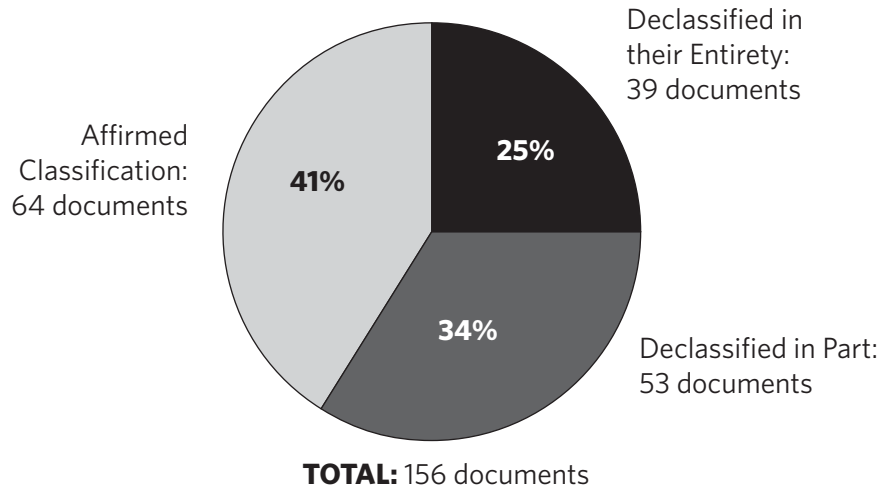
<http://www.archives.gov/isoo/oversight-groups/iscap>

Number of Appeals Received by ISCAP

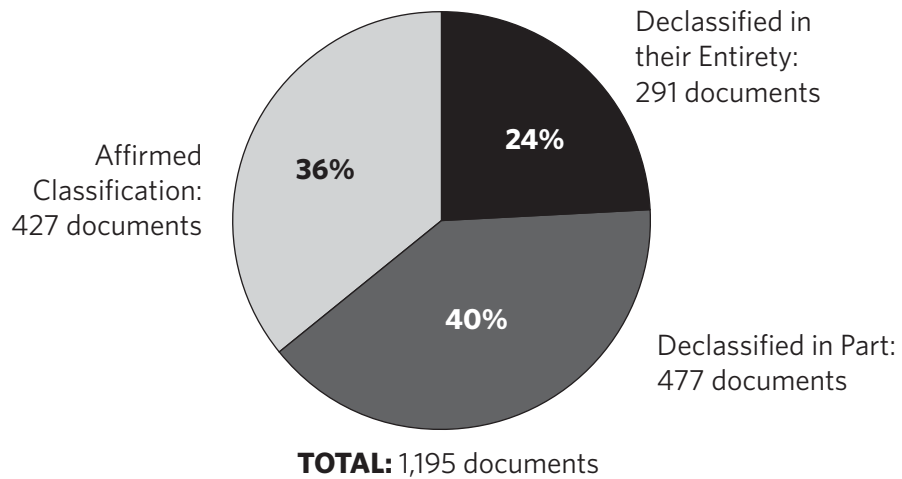


INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

ISCAP Decisions, FY 2011



ISCAP Decisions, May 1996 - September 2011



NATIONAL INDUSTRIAL SECURITY PROGRAM

ISOO is responsible for implementing and overseeing the National Industrial Security Program (NISP) under E.O. 12829, as amended, issued in 1993. This oversight responsibility is primarily executed through the National Industrial Security Program Policy Advisory Committee (NISPPAC), a Federal Advisory Committee organized pursuant to section 103 of E.O. 12829, as amended. Membership of the NISPPAC is comprised of both Government and industry representatives, and the NISPPAC is chaired by the Director of ISOO.

The NISPPAC advises on all matters involving the policies of the NISP and is responsible for recommending changes to industrial security policy, specifically E.O. 12829, as amended, its implementing directive (32 CFR part 2004), and the National Industrial Security Program Operating Manual (NISPOM). The NISPPAC convenes at least twice a calendar year at the discretion of the NISPPAC Chair, and the meetings are open to the public in accordance with the Federal Advisory Committee Act.

During FY 2011, the NISPPAC held three meetings, one of which was held in conjunction with the annual training seminar of the National Classification Management Society, providing personnel an opportunity to view the workings of the NISPPAC and to meet

those representing them and their agencies on the Committee. The following issues were presented and discussed: personnel security clearance (PCL) processing; certification and accreditation of information systems; foreign ownership, control or influence of NISP facilities; reporting requirements concerning intrusions to unclassified information systems; status and plan for eliminating security containers not approved by the General Services Administration, industry access to threat data; and the on-going revision of the NISPOM.

The two working groups formed in FY 2008 met to address NISPPAC action items and issues of mutual interest. The PCL working group reviewed and analyzed a comprehensive set of metrics that measure the timeliness of PCL processing for industry. The analysis of these metrics resulted in the identification and implementation of suggested improvements to the PCL process, as well as the formation of an ad-hoc working group to look

The National Industrial Security Program (NISP) is a partnership between the federal government and private industry to safeguard classified information.

specifically at the chief causes of rejections of PCL requests. Preliminary results indicate that electronic fingerprinting system capability needs to be readily available on a cost-effective basis to Government and industry to substantially minimize the current rejection rate. Likewise, the Certification and Accreditation (C&A) working group continued its review and analysis of the process for industry to obtain approval to process classified information on designated systems. This group recommended changes to standards and metrics to improve the timeliness and effectiveness of the C&A process and ensure that it is consistent with national policy.

The NISPPAC continues to work with DoD, the NISP executive agent, to update the NISPOM. A revised version will be issued in 2012.

The impact of E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," on NISP processes

NATIONAL INDUSTRIAL SECURITY PROGRAM

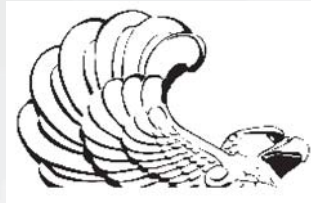
and its implementation within cleared industry is under review. This policy requirement will ensure the continuity of the mandatory structural reforms through integration into NISP processes and implementation standards by those NISP contractors, grantees, and licensees with approval to operate classified information systems.

The impact of the issuance of E.O. 13556, "Controlled Unclassified Information," (CUI), on the NISP contractors, grantees, or licensees remains an issue of discussion and concern by the NISPPAC. The inclusion of NISPPAC industry representatives in CUI implementation efforts will ensure its successful continuity

and integration into NISP processes and implementation standards.

Information on the NISPPAC is available on the ISOO website <http://www.archives.gov/isoo/oversight-groups/nisppac>





INFORMATION SECURITY
OVERSIGHT OFFICE



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