ANNUAL REPORT TO THE PRESIDENT

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

2012

INFORMATION SECURITY OVERSIGHT OFFICE

Annual Report to the President

INFORMATION SECURITY OVERSIGHT OFFICE • NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

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"
- 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.

ISOO's Mission

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest. We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

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.
- 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.
- Serve as 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.

ON THE COVER: Pennsylvania Avenue Entrance, 1942

Letter to the President

June 20, 2013

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 2012, as required by Executive Order 13526, "Classified National Security Information" (the Order).

This report provides statistics and analysis of the system of classification and declassification based on ISOO's review of Departments' and Agencies' programs, including agency self-reporting. 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."

This year, we have incorporated our cost report on security classification activities into this consolidated annual report. Overall, reported costs for Government and industry combined are $10.96 billion. This is a decrease from last year of $1.66 billion, or 13 percent.

Agencies completed the first executive branch-wide Fundamental Classification Guidance Review in FY 2012, a major investment in combating over-classification and limiting secrecy to only that information truly necessary to protect the national security. Twenty-five agencies with original classification authority conducted comprehensive reviews of their classification guidance, streamlining and consolidating 3,103 classification guides, to reflect current circumstances.

ISOO also completed its five-year on-site assessment of agency declassification programs. This oversight and assistance program garnered significant measureable improvements in the quality of declassification reviews conducted by departments and agencies across the executive branch. ISOO will continue its assessment program in a form that sustains this high level of quality.

ISOO continues to develop and refine its ability to monitor agency efforts at self-assessment. For two years we have worked vigorously to help agencies improve the coverage and quality of their self-inspection programs, as required by the Order. ISOO's analysis of these efforts also contributes to the White House Senior Information Sharing and Safeguarding Steering Committee's annual report to you.

The Interagency Security Classification Appeals Panel (the Panel) continued adjudicating declassification appeals while also launching a new web site that makes declassified documents publically available. The collection of documents now online fulfills the Order's requirement that the Panel inform senior agency officials and the public of its decisions on mandatory declassification review appeals and classification challenges. This tool is now available to agencies to help them conduct more consistent and accurate declassification reviews.

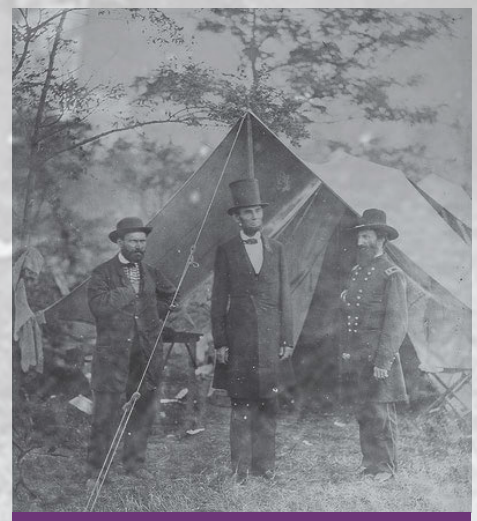
The National Industrial Security Program Policy Advisory Committee (NISPPAC) made meaningful improvements in the areas of personnel security clearances and certification and accreditation of information systems. Importantly, by improving linkages with the Office of the Director of National Intelligence in its government-wide role as Security Executive Agent, NISPPAC is better able to monitor and characterize the industry experience in the government-wide security clearance process. The NISPPAC continues to ensure the requirements for the protection of classified information by the private sector are consistent with those established by the Order.

Respectfully,

JOHN P. FITZPATRICK
Director

Table of Contents

Summary of FY 2012 Program Activity



Classification

- Executive branch agencies reported 2,326 original classification authorities (OCA), down from 2,362 reported in FY 2011.
- Agencies reported 73,477 original classification decisions, a decrease of 42 percent.
- Agencies reported using the ten-years-or-less declassification instruction for 48 percent of original classification decisions.
- Executive branch agencies reported 95,180,243 derivative classification decisions; a 3 percent increase from FY 2011. This increase reflects revised reporting requirements intended to better capture classification activity in the electronic environment.

Declassification

- Agencies received 7,589 initial mandatory declassification review (MDR) requests and closed 6,533 requests. The average number of days to resolve each request is 228. A total of 6,666 requests have remained unresolved for over one year. This number includes requests that have been carried over from prior years.
- Agencies reviewed 372,354 pages under MDR, and declassified 217,456 pages in their entirety, declassified 86,587 pages in part, and retained classification of 68,311 pages in their entirety.
- Agencies received 368 MDR appeals and closed 321 appeals. The average number of days to resolve each appeal is 240. A total of 233 appeals have remained unresolved for over one year.
- Agencies reviewed 10,920 pages on appeal, and declassified 3,173 pages in their entirety, declassified 3,442 pages in part, and retained classification of 4,305 pages in their entirety.
- Under automatic declassification, agencies reviewed 39,906,554 pages and declassified 17,694,016 pages of historically valuable records.
- Under systematic declassification reviews, agencies reviewed 4,168,395 pages, and declassified 1,977,339 pages.
- Under discretionary declassification reviews, agencies reviewed 846,915 pages, and declassified 179,186 pages.
- Under automatic, systematic, and discretionary declassification reviews, a total of 44,921,864 pages were reviewed for declassification and 19,850,541 pages were declassified.

A Note About Future Reports:

As reported in FY 2011, ISOO continues to work with agencies to re-evaluate how best to measure and report accurate and meaningful data reflecting the classification and declassification activity across Government. ISOO continues to seek improved measuring and reporting methods to better oversee the Government's classification and declassification programs.

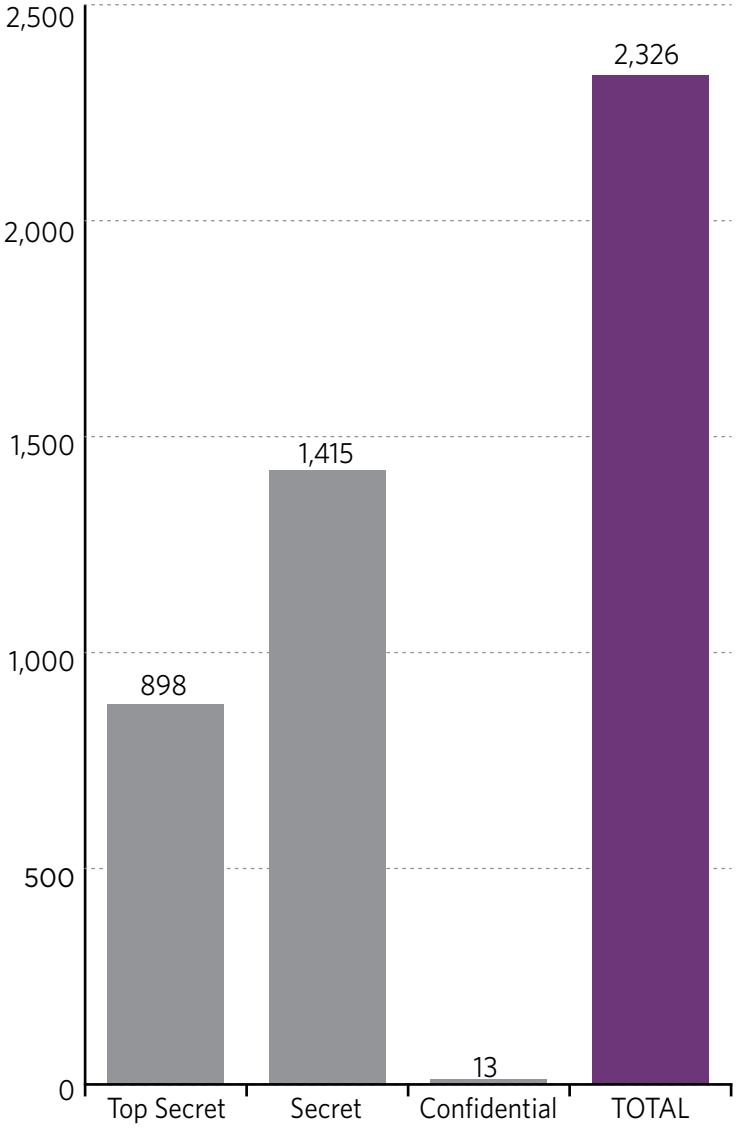
In FY 2012, ISOO implemented a new reporting requirement to measure the response time for mandatory declassification review (MDR) requests. Agencies now report the average number of days it takes for them to close MDR requests. Agencies and ISOO can more clearly understand how agencies are executing their MDR programs successfully by comparing average response times, data previously not studied. Agency response times will be analyzed to identify trends within an agency's program and across agencies of comparable size. We believe this method presents a clearer picture of the MDR response situation at an agency than the previous reporting method of measuring the number of cases outstanding from the previous fiscal year, the number of new cases requested, and the number of cases to be carried into the new fiscal year.

Classification

Original Classification Authorities

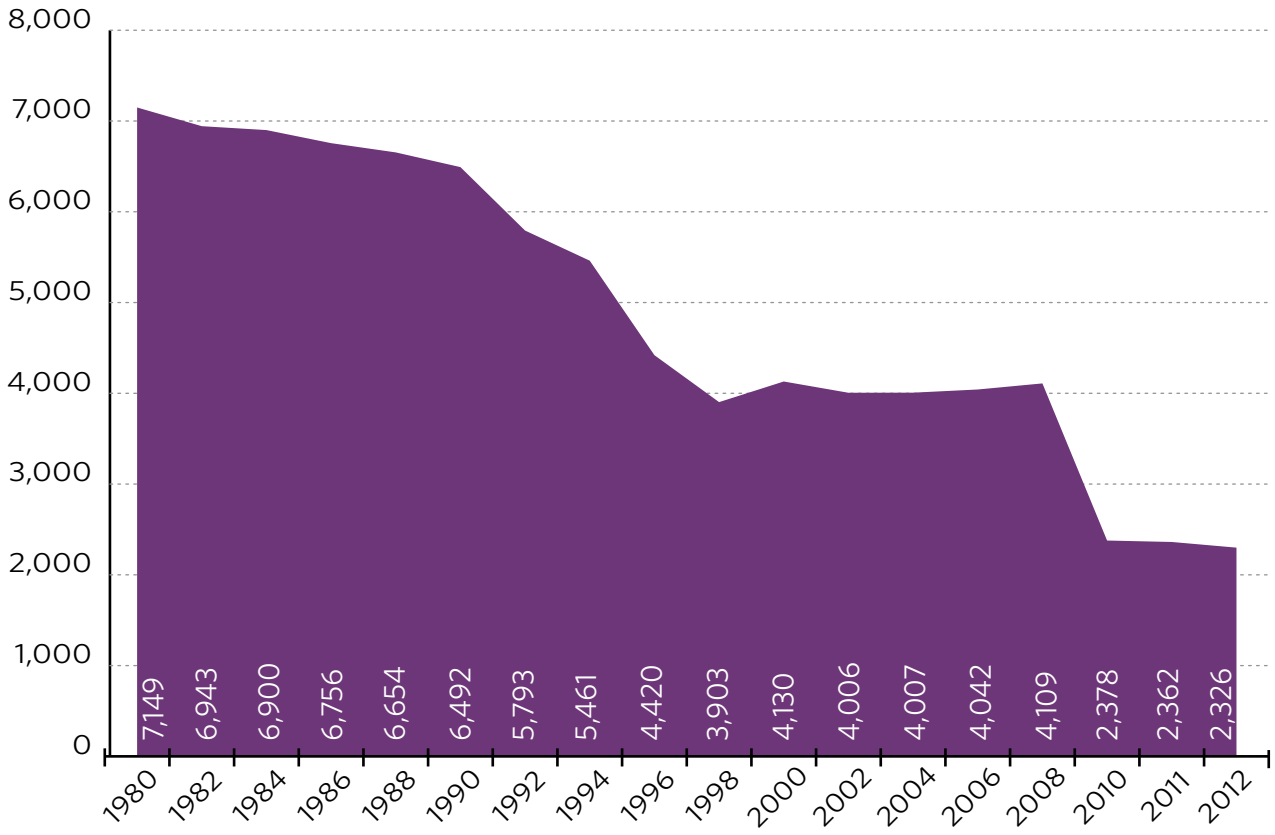
Original classification authorities, also called original classifiers, are those individuals designated in writing, either by the President, by selected agency heads, or by designated senior agency officials with Top Secret original classification authority, to classify information in the first instance. 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 2,326 OCAs in FY 2012; a .02 percent decrease from the 2,362 reported in FY 2011.

Original Classification Authorities, FY 2012



Inauguration of John F. Kennedy, January 20, 1961

Number of Original Classification Authorities, FY 1980 – FY 2012



Card Catalog in National Archives Central Search Room, 1942

Original Classification

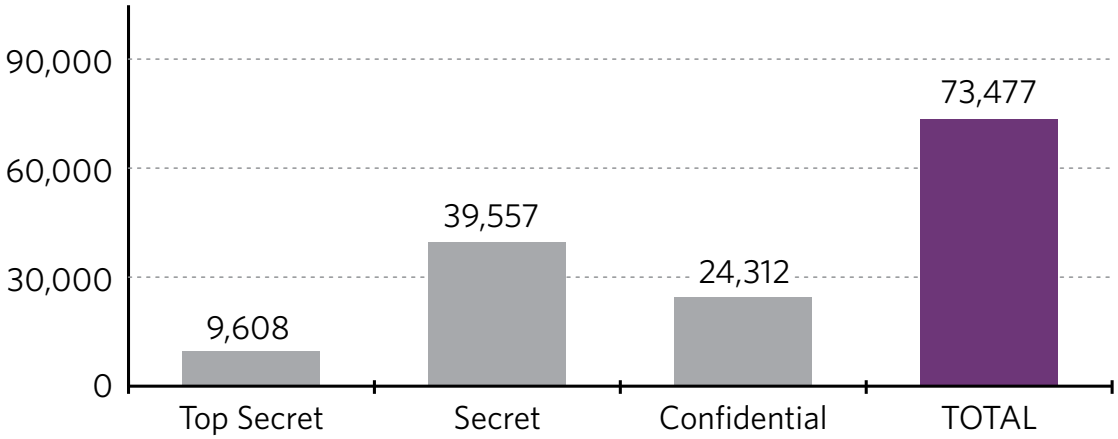
Original classification is a novel determination by an OCA that information owned by, produced by or for, or under the control of the U.S. Government requires protection because unauthorized disclosure of that information could reasonably be expected to cause damage to the national security.

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 will become declassified unless it is appropriately referred, exempted, or excluded from automatic declassification. By definition, original classification precedes all other aspects of the security classification system, including derivative classification, safeguarding, and declassification. It will be noticed that some large agencies report very few original classification decisions. This is in large part due to the fact that their classification guides are comprehensive and therefore the bulk of their classification activity is derivative classification.

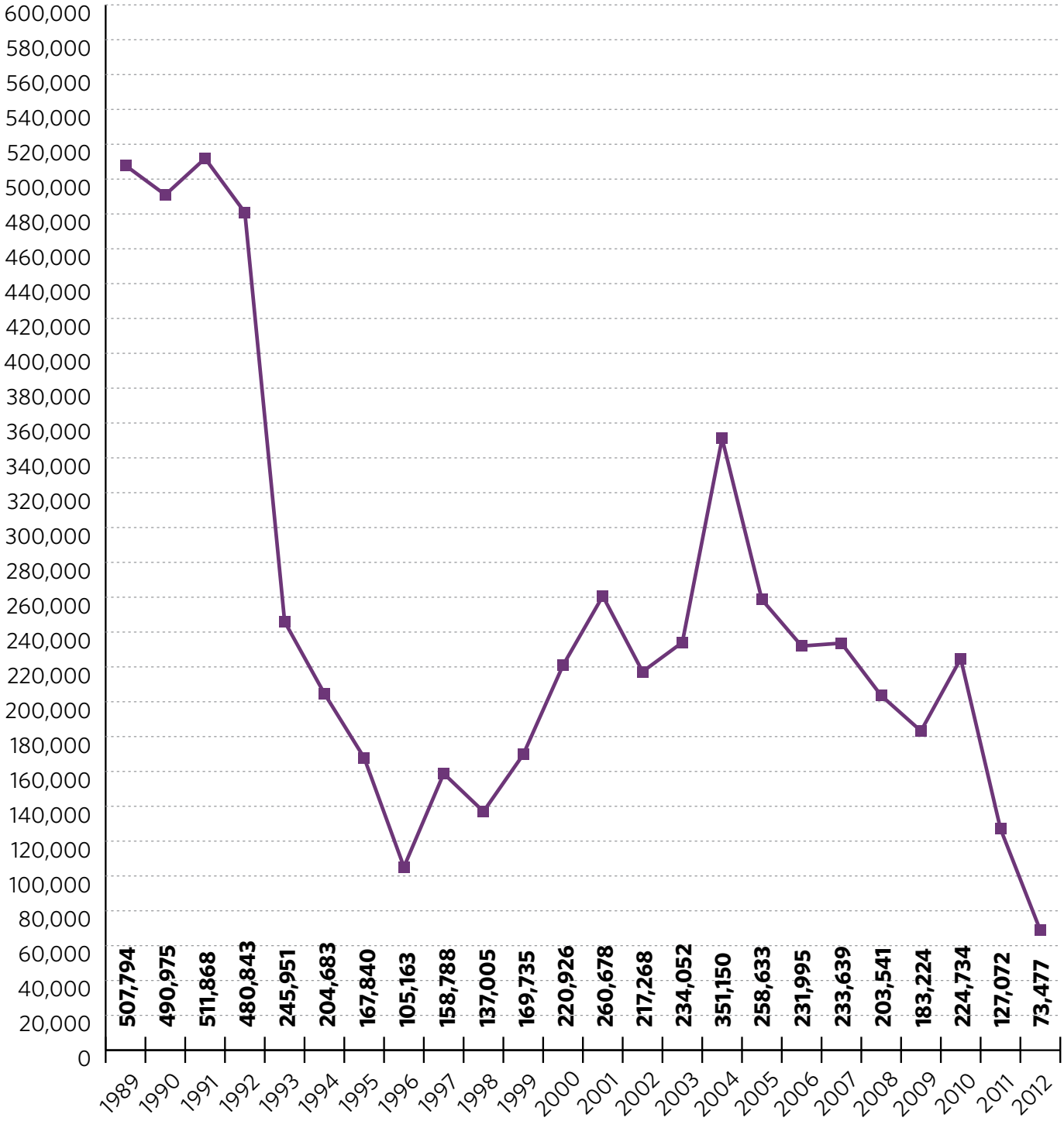
Agencies reported 73,477 original classification decisions for FY 2012, using the ten-year-or-less declassification instruction 48 percent of the time.

Agencies decreased their total number of original classification decisions by 42 percent during FY 2012, a result attributed in part to the conduct of the Fundamental Classification Guidance Review (FCGR). The FCGR entailed the re-evaluation of the accuracy of agency security classification guides in an effort to ensure proper and standardized classification of information vital to national security across Government. Accurate and current security classification guides also expedite declassification by avoiding over-classification and unnecessary withholding of records. Additionally, many agencies reviewed their requirements and need for OCAs while conducting the FCGR, resulting in a total decrease of 36 OCAs across agencies (*http://www.archives.gov/isoo/fcgr/index.html*).

Original Classification Activity, FY 2012



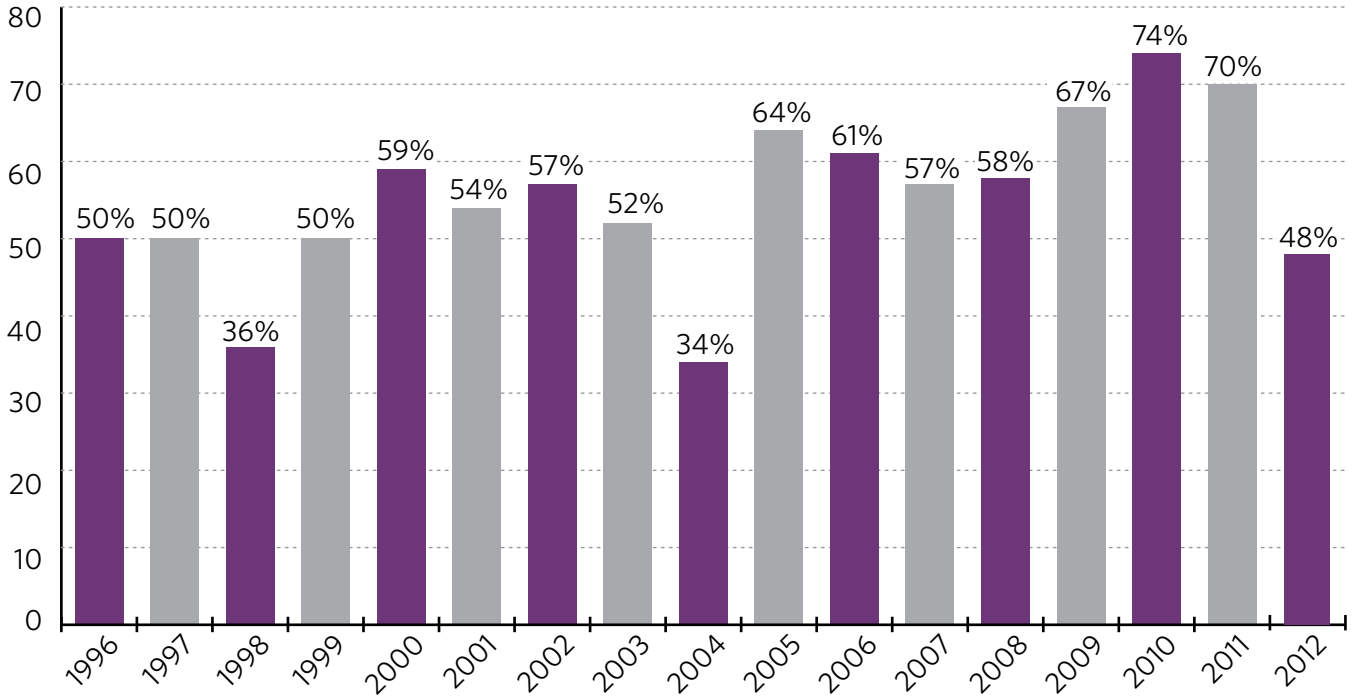
Original Classification Activity, FY 1989 – FY 2012



Original Classification Activity by Agency, FY 2012

Agency	Total Activity
Department of State	39,770
Department of Defense	19,121
Department of the Navy	4,958
Department of Justice	4,689
Executive Office of the President	2,476
Department of the Army	2,399
Department of Homeland Security	40
Office of the Director of National Intelligence	8
Central Intelligence Agency	4
Millennium Challenge Corporation	4
Department of the Treasury	4
Department of Commerce	2
Department of the Air Force	1
Environmental Protection Agency	1
Total	**73,477**

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 identify elements of information regarding a specific subject that must be classified and establish the level and duration of classification for each such element.

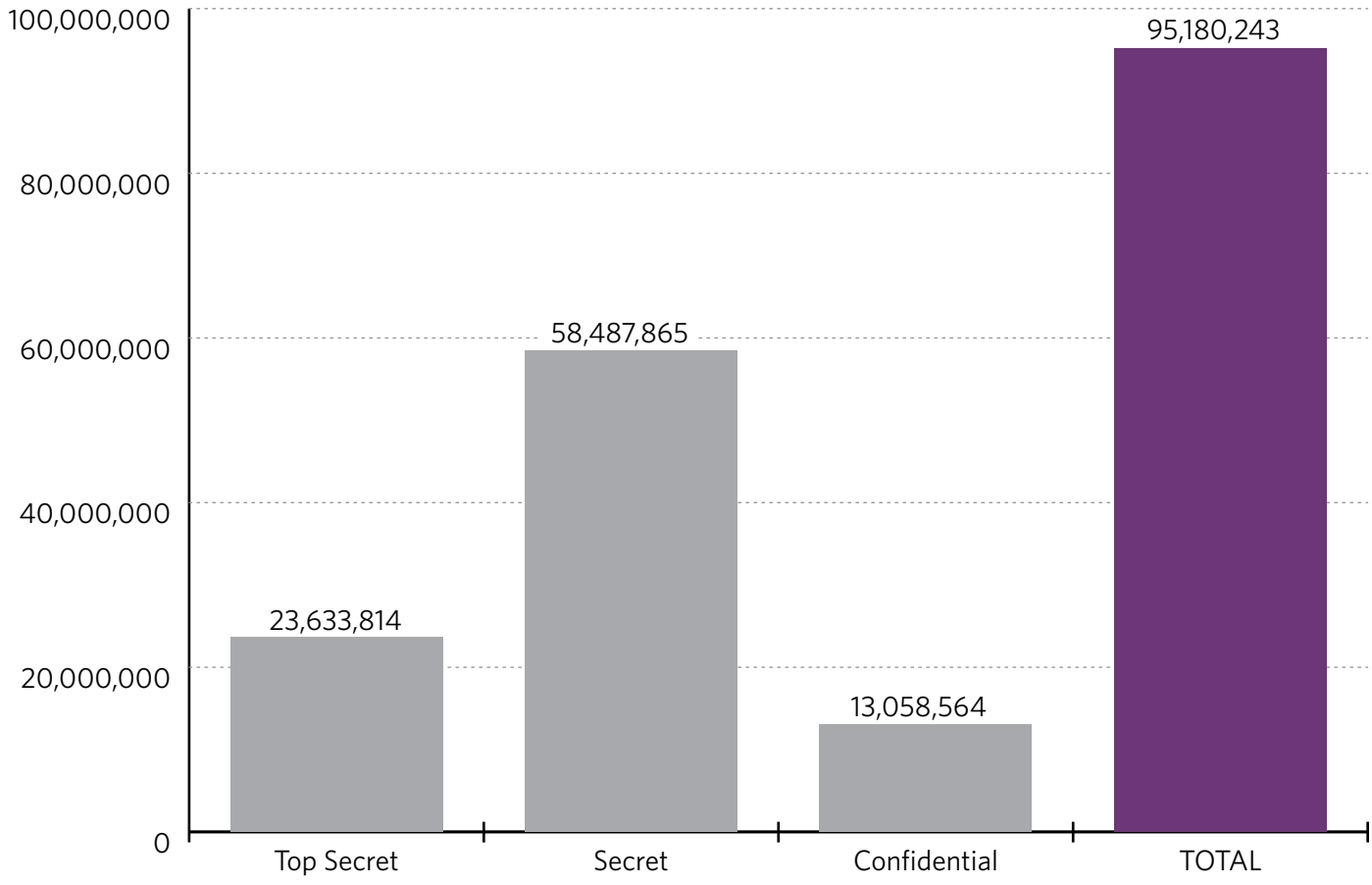
Derivative classification actions utilize information from the original category of classification.

Every derivative classification action is based on information where classification has already been determined by an OCA. Derivative classification decisions must be traceable to the original classification decision made by an OCA.

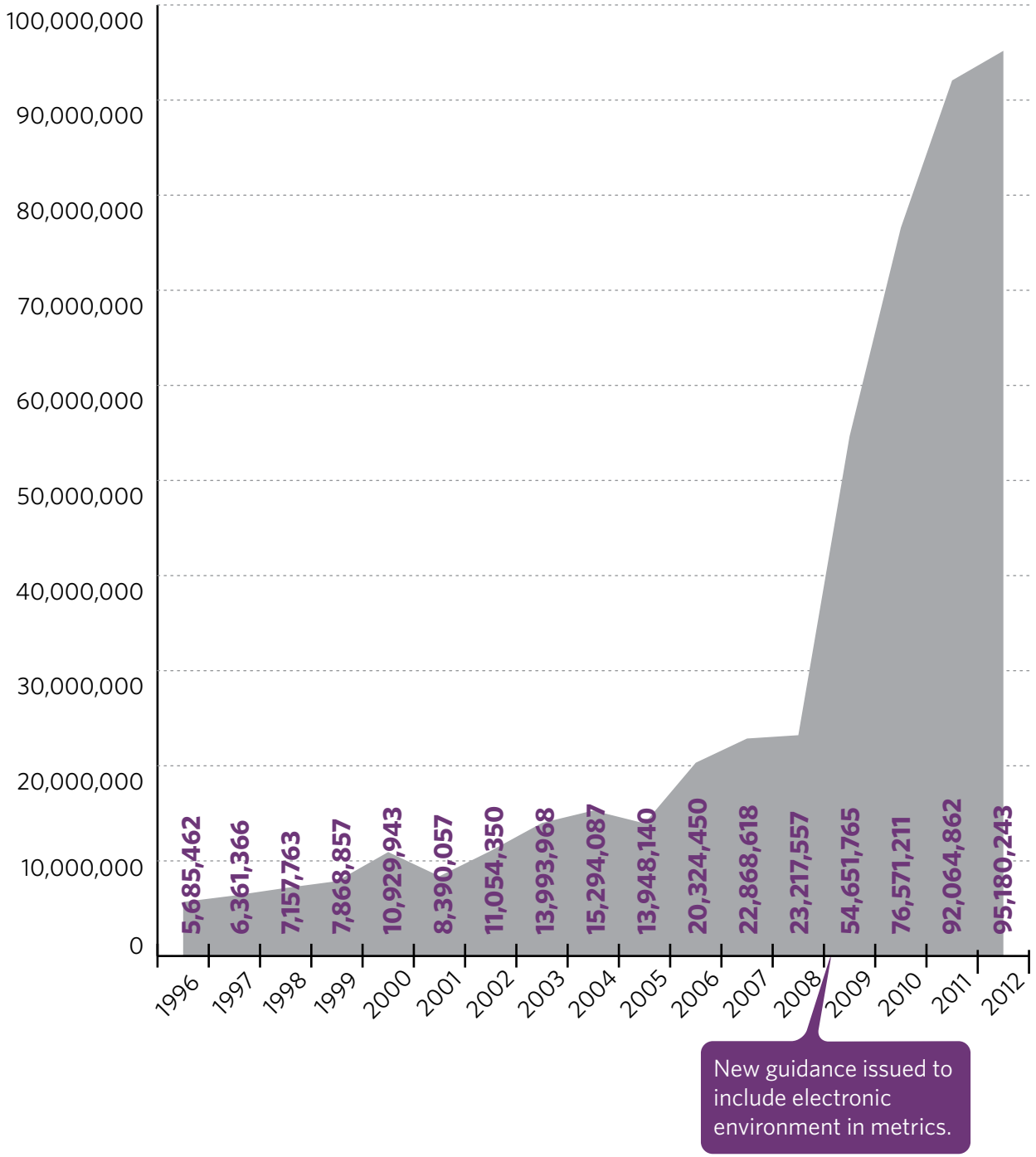
Agencies reported a total of 95.2 million derivative classification decisions in FY 2012. In FY 2009, ISOO issued new guidance that asked agencies to focus on counting classification decisions in the electronic environment to account for the expanded methods of classified communications (e.g. e-mail, classified web pages, blogs, wikis, bulletin boards, instant messaging, etc.) Agencies continue to report annual growth in the number of derivative decisions based on this new guidance.

Examination of a new photo accession, circa 1940

Derivative Classification Activity, FY 2012



Derivative Classification Activity, FY 1996 – FY 2012



Classification Challenges

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. Classification challenges provide a mechanism to promote sound classification decisions.

Agencies reported 402 formal challenges in FY 2012; 266 (66.2 percent) were fully affirmed at their current classification status with 126 (31.3 percent) being overturned either in whole or in part. Ten challenges remain open.

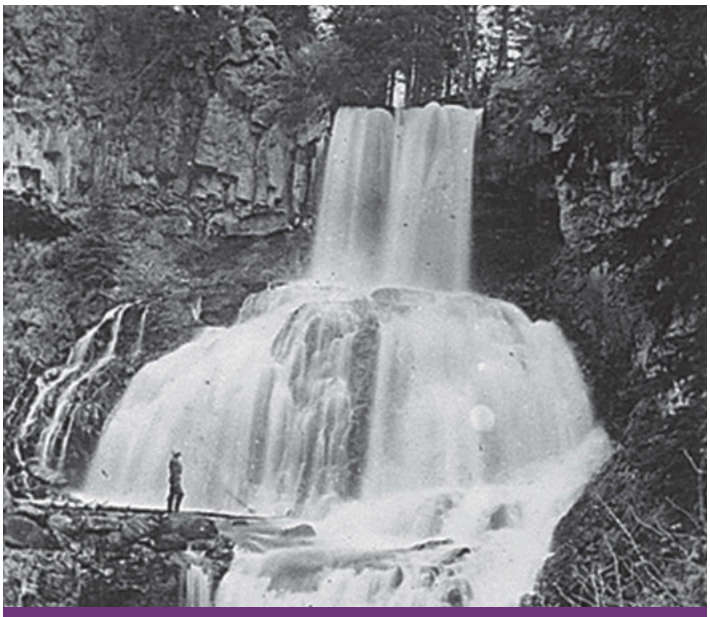
Declassification

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 direct, specific review for declassification of information when requested by the public.

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, agencies began to report automatic, systematic, and discretionary declassification numbers separately. Together, these four programs are essential to the viability of the classification system and vital to an open government.



Gardiner Falls, Yellowstone National Park, circa 1874

Automatic, Systematic, and Discretionary Declassification Review

During FY 2012, a total of 44.92 million pages were reviewed under the automatic, systematic, and discretionary declassification programs and 19.85 million pages (44 percent) were declassified*. This is a 7 percent decrease in the scale of declassification from FY 2011, when 52.76 million pages were reviewed and 26.72 million pages (51 percent) were declassified.

In FY 2012, agencies reviewed nearly 8,000,000 fewer pages under automatic, systematic, and discretionary declassification reviews than in FY 2011. There were numerous factors contributing to this decline. The majority of the reductions were in the automatic declassification reviews. A change in contractors, a temporary inability to access and review records at the Washington National Records Center, and the relocation of facilities all contributed to fewer pages being reviewed for declassification. Additionally, agencies systematically reviewed a large volume of records (an entire file series) for declassification in FY 2011, causing a spike in that year's total. This large, one-time declassification review was a directed tasking for FY 2011 and was truly an exceptional case. An equivalent declassification tasking did not occur in FY 2012.

In previous annual reports, ISOO attributed the high annual declassification totals of the late 1990s to agency reviews of large volumes of classified records spanning multiple decades (1940 through 1981) in anticipation of the first onset of the automatic declassification program. These automatic declassification numbers will likely not occur again as agencies need only to identify and review those records newly subject to automatic declassification at the end of the 2012 calendar year. The number of records subject to automatic declassification may vary as the process for identifying and reviewing records is dependent on agency records management practices, the complexity of the reviews, and agency resources.

Under automatic declassification review, agencies reviewed 39.91 million pages and declassified 17.69 million pages. This result is a decrease of 8 percent in pages declassified from FY 2011.

Under systematic declassification review, agencies reviewed 4.17 million pages and declassified 1.98 million page. This result is an increase of 1 percent in pages declassified from FY 2011.

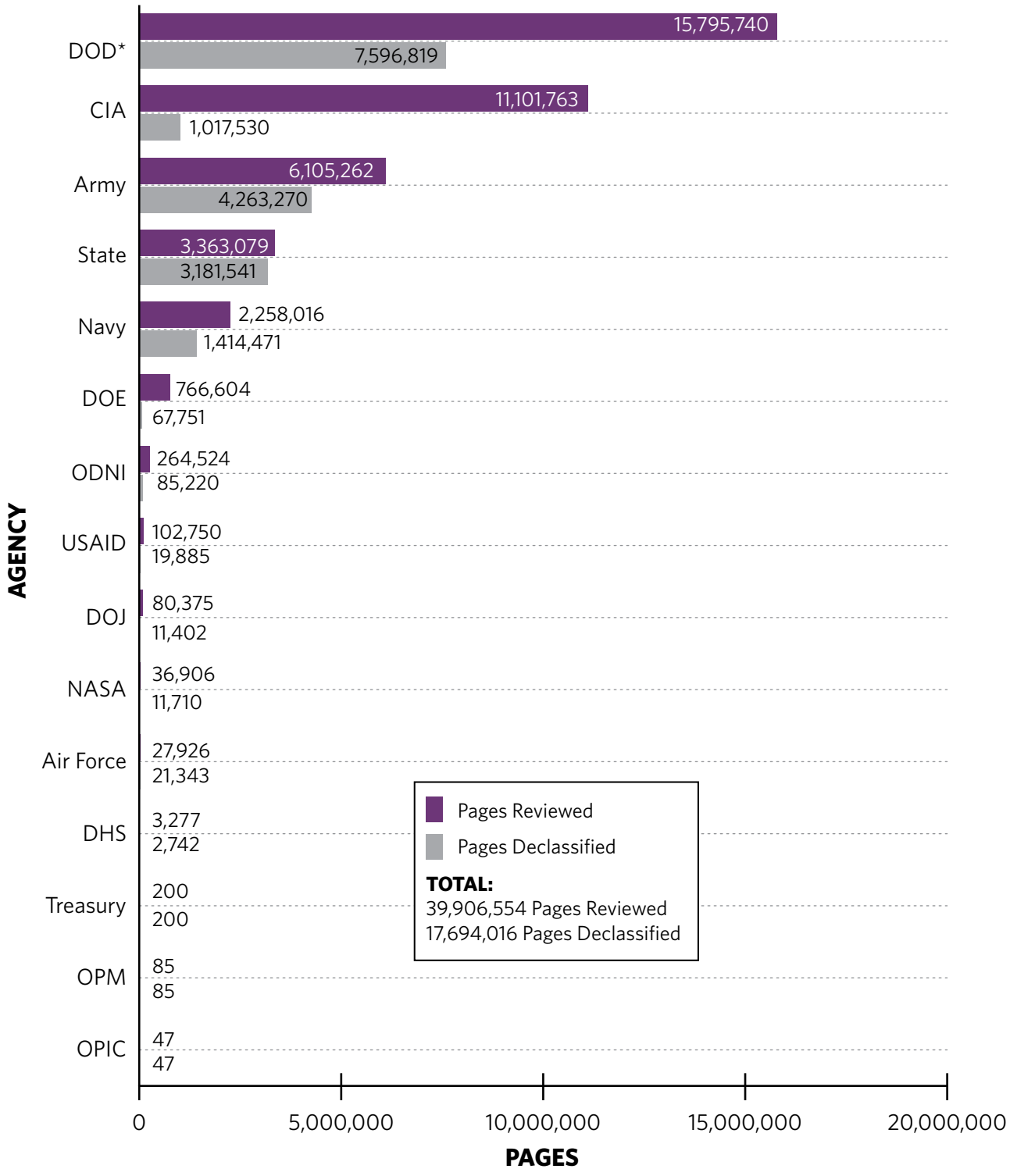
Under discretionary declassification review, agencies reviewed 846,915 pages and declassified 179,186 pages. This result is an increase of 45 percent from FY 2011.

As a note of explanation, in the following four charts it can be seen that some agencies have a low rate of pages declassified compared to the total number of pages reviewed. In many cases, this is because the bulk of the information in these pages contained equities from other agencies and therefore had to be referred to those agencies.

** This data does not include the status of the backlog processed by the National Declassification Center. Information about that program can be found at http://www.archives.gov/declassification/ndc/releases.html*

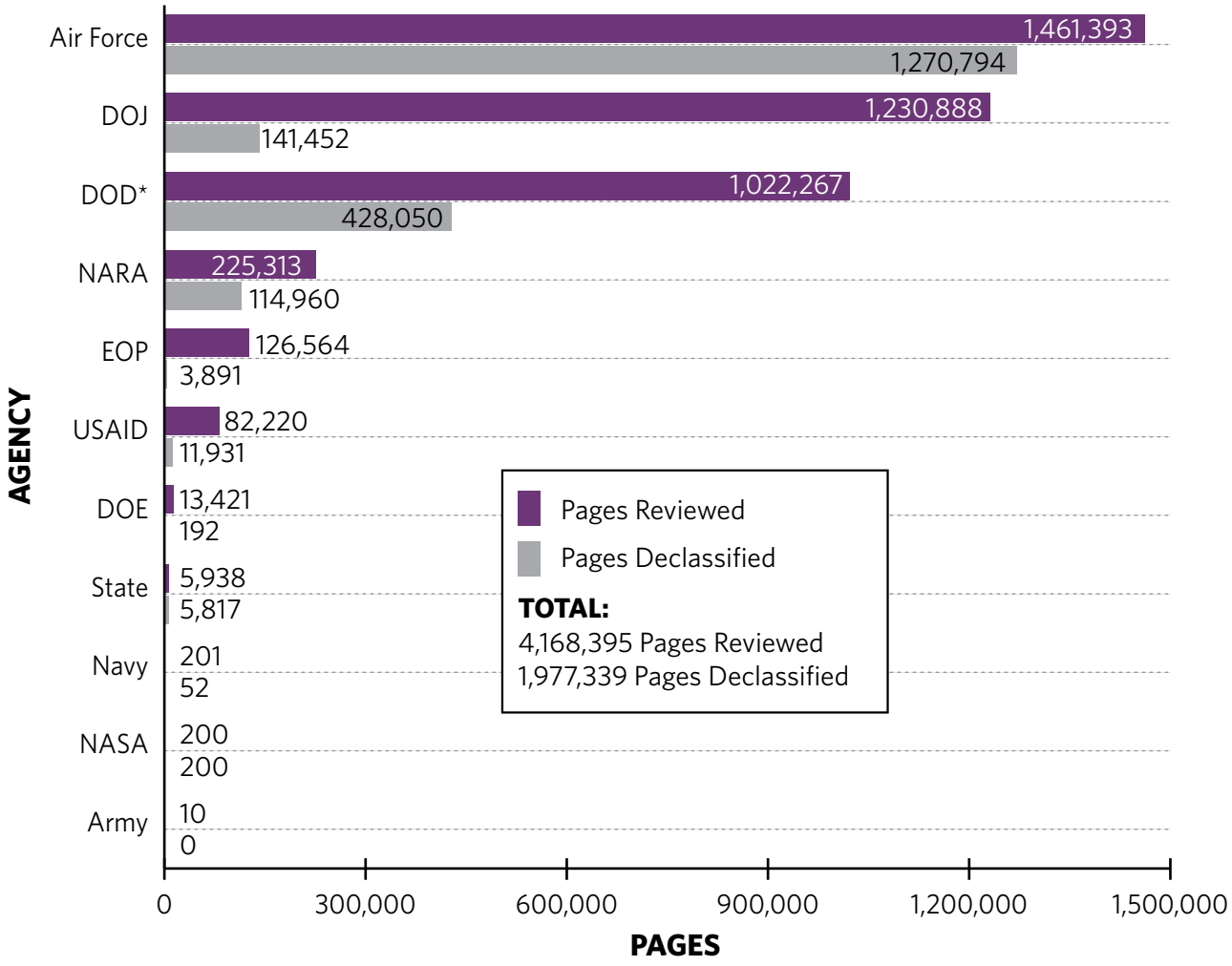
President Truman receiving a Thanksgiving turkey from members of the Poultry and Egg National Board and other representatives, outside the White House, November 16, 1949

Number of Pages Reviewed and Declassified for Automatic Declassification, *FY 2012*



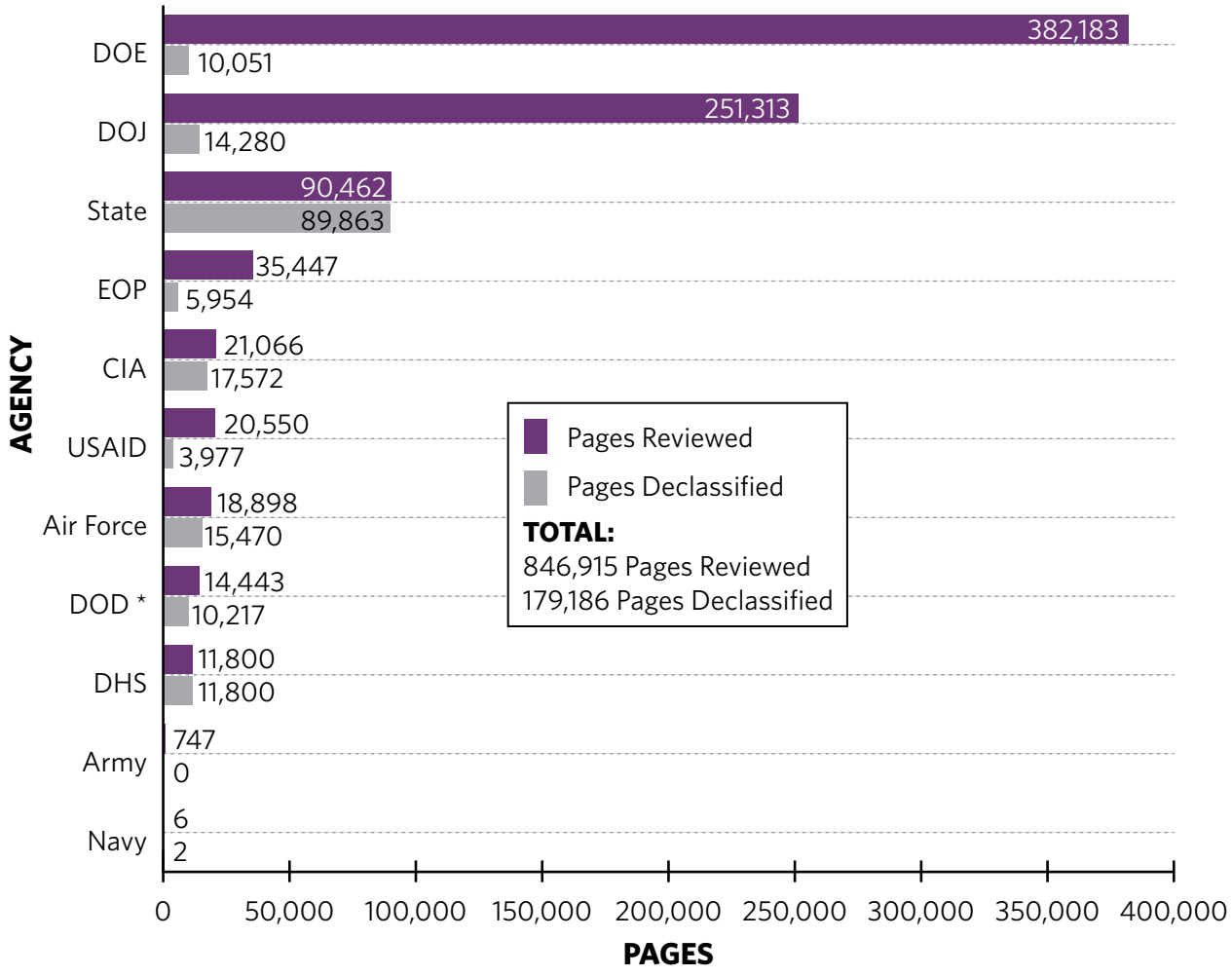
** Does not include Air Force, Army, and Navy.*

Number of Pages Reviewed and Declassified for Systematic Declassification, *FY 2012*



** Does not include Air Force, Army, and Navy.*

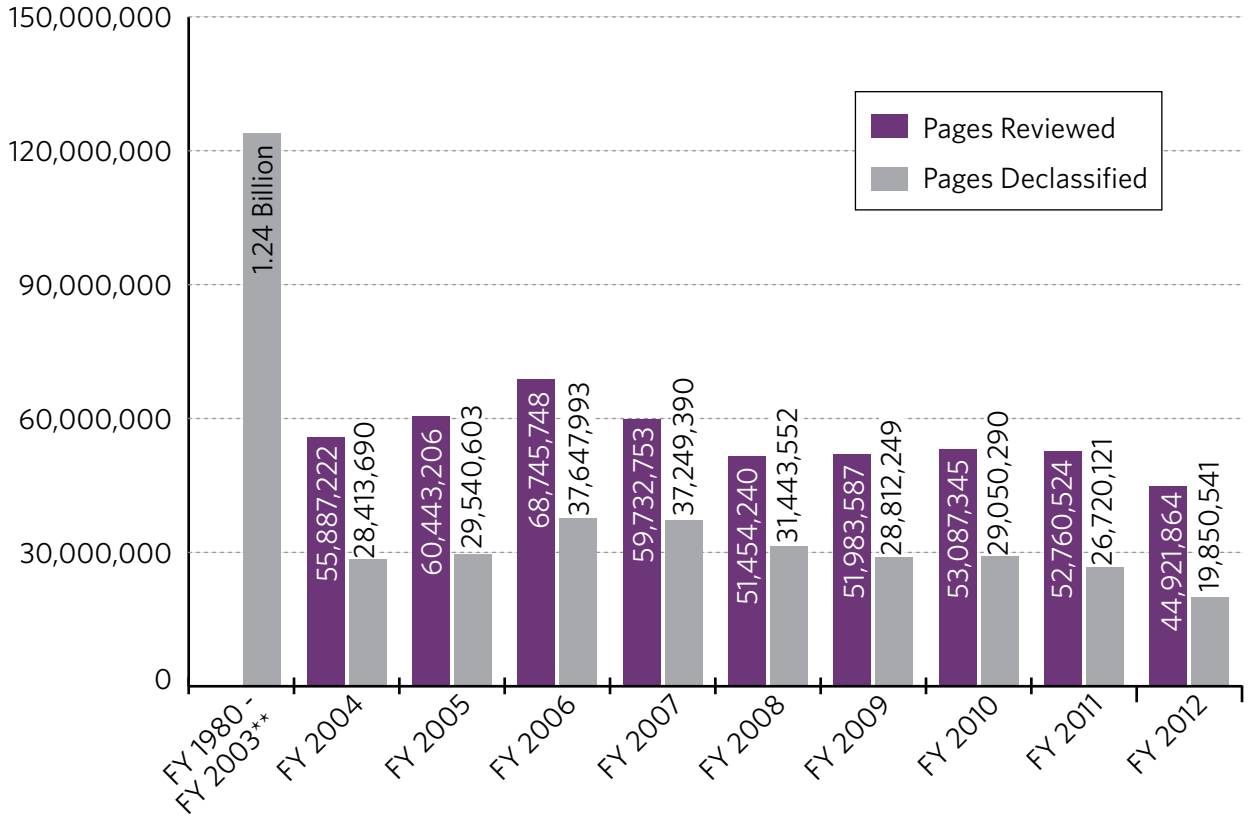
Number of Pages Reviewed and Declassified for Discretionary Declassification, *FY 2012*



** Does not include Air Force, Army, and Navy.*

Total Number of Pages Reviewed and Declassified, FY 1980 – FY 2012*

(Automatic, Systematic, and Discretionary Declassification Reviews)
1.51 Billion Pages Declassified



** Excluding Mandatory Declassification Review*
*** Number of pages reviewed not available*

Mandatory Declassification Review

The mandatory declassification review (MDR) process requires a review of specific classified national security information in response to a request seeking its declassification. The public must make MDR requests in writing and each request must contain sufficient specificity describing the record to allow an agency to locate the record 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.

In FY 2012, ISOO implemented a new reporting requirement to measure the response time for MDR requests. Agencies now report the average number of days it takes for them to close MDR requests. Agencies and ISOO can more clearly understand how agencies are executing their MDR programs successfully by comparing average response times, data previously not studied. Agency response times will be analyzed to see trends within an agency's program and across agencies of comparable size. We believe this method presents a clearer picture of the MDR response situation at an agency than the previous reporting method of measuring the number of cases outstanding from the previous fiscal year, the number of new cases requested, and the number of cases to be carried into the new fiscal year.

MDR Activity, FY 2012

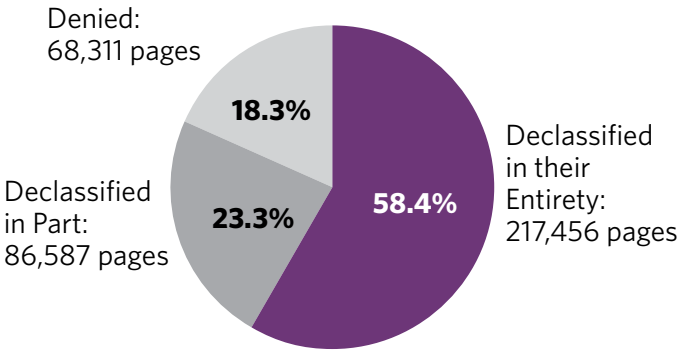
The FY 2012 data specify the number of requests and appeals received, the number that remain unresolved for over one year, and the average number of days it takes to resolve each request and appeal. For the first time, the report displays the number of referred MDR requests and appeals to more accurately reflect the MDR workload of agencies. The number of referred MDR requests and appeals are not included in the statistical calculations to prevent duplicate counts.

MDR Program Activity, FY 2012

Requests Received	7,589
Requests Closed	6,533
Requests Unresolved for Over One Year	6,666
Average Number Days to Resolve Each Request	228
Appeals Received	368
Appeals Closed	321
Appeals Unresolved for Over One Year	233
Average Number Days to Resolve Each Appeal	240
Referred Requests Received*	10,001
Referred Appeals Received*	212

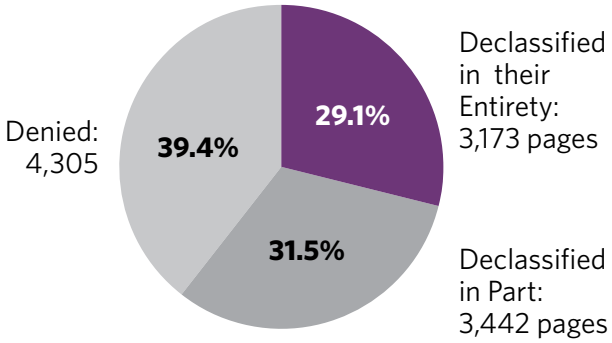
** MDR requests and appeals referred to an agency from another agency that is responsible for the final release of the request/appeal.*

Disposition of MDR Requests, FY 2012



TOTAL: 372,354 pages

Disposition of MDR Appeals, FY 2012



TOTAL: 10,920 pages

Reviews

Declassification Assessments

In FY 2012, ISOO continued to evaluate the proficiency of agencies' automatic declassification review programs. ISOO disseminated the results of its evaluations to the agencies for the purpose of strengthening their programs, identifying best practices and correcting common errors in the declassification community as a whole. Using Standard Form (SF) 311, Agency Security Classification Management Program Data, submission data from FY 2011, ISOO identified agencies with declassification programs substantial enough to warrant assessment. ISOO contacted each agency and asked for information on bodies of records reviewed for declassification during the previous six-month period. 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 16 agencies during FY 2012.

Assessments focused on three areas of concern: missed equities, inappropriate referrals, and improper exemptions.

- Missed equities indicated instances of a review not identifying for referral the security classification interest of one agency found in the record of another agency
- Inappropriate referrals denoted instances of a review resulting in the referral of records to agencies lacking the authority to exempt information from declassification or waiving their interest in the information.
- Improper exemptions included instances of a review resulting in an attempt to exempt a record from automatic declassification under an exemption category not permitted by the agency's declassification guide as

Delegation of officers of the National American Woman Suffrage Association received by President Woodrow Wilson, 1917

approved by the Interagency Security Classification Appeals Panel (ISCAP).

ISOO analysts factored the occurrence of any of these three issues into the overall agency score for the assessment. 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 one instance of an inappropriate referral. ISOO did not identify any instances of improper exemptions or missed equities in agency samples. In evaluating the various programmatic aspects of agencies' automatic declassification review programs, ISOO noted several areas of improvement.

- Agencies are reviewing appropriate records between 20–25 years of age.
- Agencies are also appropriately using the SF 715, Declassification Review Tab. Use of the SF 715 aids the standardization of declassification review determinations and helps facilitate the processing of referrals, as well as overall archival processing, of records.
- Agencies are making more informed referrals. ISOO did not identify any instances of an agency inappropriately making a referral based on letterhead instead of the content of the information in a record.

ISOO recorded the results of these assessments and scored each agency's program. 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 16 agencies assessed, 15 received scores of 90 or above while one agency received a score of 88.

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.

Declassification Assessment Results, FY 2012

Agency	Result
Central Intelligence Agency	100
Defense Threat Reduction Agency	100
Department of State	100
Department of the Air Force	100
Federal Bureau of Investigation	100
Joint Staff	100
Missile Defense Agency	100
National Geospatial-Intelligence Agency	100
Office of the Secretary of Defense	100
National Security Agency	98
Department of the Army	96
Defense Intelligence Agency	94
U.S. Agency for International Development	94
Department of Energy	92
National Archives and Records Administration	90
Department of the Navy	88

Declassification Assessment Results, FY 2008 – FY 2012

Fiscal Year	Number of Agencies	Average Score
2008	22	79
2009	19	84
2010	15	90
2011	15	94
2012	16	97

Bluffs on the head of the West Gallatin, about 60 miles above the mouth of the canyon, Yellowstone, 1872

Fundamental Classification Guidance Review (FCGR)

In 2009, President Obama tasked all executive branch agencies with classification authority to conduct comprehensive Fundamental Classification Guidance Reviews (FCGR). The purpose of these reviews was to ensure that guidance reflects current circumstances as to what information warrants continued classification. Additionally, the reviews identified information that no longer requires classification and can be expedited for declassification. The review helped agencies ensure proper classification of information vital to national security, while avoiding over-classification and unnecessary classification of records.

The reviews were systematic, comprehensive, and conducted with thoughtful scrutiny involving detailed data analysis. The agencies completed the FCGR in June 2012 with the result of 3,103 classification guides reviewed, and 869 either cancelled or consolidated. Additionally, agencies eliminated, revised, consolidated, or condensed numerous projects, programs, and categories of information. Agencies will conduct the FCGR every five years; the next review will be completed in 2017.

Review highlights include:

- The Department of Energy cancelled unnecessary guides, deleted redundancy, reduced the number of subjects exempted from automatic declassification, and replaced erratic declassification events with fixed declassification dates in its guidance.

- The National Reconnaissance Office created an Integrated Classification Guide to standardize classification requirements agency-wide and improve efficient and timely declassification guidelines and processes.

- The Environmental Protection Agency developed its first agency classification guide.

- The Department of the Navy implemented a Security Classification Guide Management System to provide horizontal comparison of classification across all guides. The system identifies classification inconsistencies and establishes a classification baseline.

- The Department of Justice created five classification guides covering classified information in the Criminal and National Security Divisions.

- The Defense Intelligence Agency determined its exact number of active guides, thereby gaining better accountability over its classification program.

Agencies decreased the total number of original classification decisions during FY 2012 by 42 percent. A large part of this decrease can be attributed to the FCGR process and the appropriate recording of classification decisions in security classification guides. Additionally, many agencies reviewed their requirements for OCAs during the review and were able to decrease the total number by 36.

Each agency that participated in the FCGR provided ISOO with a summary report of their review, which ISOO posted on its web site at *http://www.archives.gov/isoo/fcgr/index.html*.

Self-inspections evaluate the effectiveness of agency programs covering original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight.

Self-Inspections

E.O. 13526, "Classified National Security Information," requires agencies to establish and maintain ongoing self-inspection programs and report to the Director of ISOO on those programs each year. Self-inspections evaluate the effectiveness of agency programs covering original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight. In addition, self-inspections include regular reviews of representative samples of agencies' original and derivative classification actions; these samples must encompass all agency activities that generate classified information, and appropriate agency officials must be authorized to correct misclassification actions.

Effective self-inspection programs generally correlate to effective classified national security information (CNSI) programs. Agencies without self-inspection programs, or with weak self-inspection programs, fail to utilize an important tool for self-evaluation and are at greater risk of having unidentified deficiencies in their CNSI programs. Agencies must provide Senior Agency Officials with an evaluation of their agency's CNSI program to ensure an effective program.

The implementing directive for E.O. 13526, 32 CFR part 2001, requires the agency self-inspection reports include: (1) a description of the agency's self-inspection program that provides an account of activities assessed, program areas covered, and methodology utilized; and (2) information gathered through the agency's self-inspection program, which must include an assessment and a summary of the findings from the self-inspection program; specific information from the review of the agency's original and derivative classification actions; actions taken or planned to correct deficiencies; and best practices identified during self-inspections. In addition, ISOO requires agencies to respond to several focus questions relating to key requirements of E.O. 13526, such as training and performance evaluations.

ISOO required agencies to provide specific findings with regard to security education and training requirements of E.O. 13526. Although not all agencies reported this information, ISOO received a sufficient number of answers to provide the following findings:

(1) Initial Training–93.5 percent of agencies indicated they provided all of their cleared personnel with initial training on basic security policies, practices, and criminal, civil, and administrative penalties;

(2) Refresher Training – 80 percent of agencies reported they provided all of their personnel with required annual refresher training;

(3) Training for OCAs–81.2 percent of agencies reported they provided all of their OCAs with required annual training in the proper classification and declassification of information; and

(4) Training for Derivative Classifiers – 87 percent of agencies reported they provided all of their personnel who apply derivative classification markings with training in the proper application of derivative classification principles prior to derivatively classifying and at least once every two years thereafter.

When considering all agencies, and not only those that fulfilled ISOO's security education and training reporting requirement, agencies provided 64.4 percent of agency personnel with Initial Training, 44.4 percent of agency personnel with Refresher Training, 47.4 percent of agency personnel with Training for OCAs and 47.1 percent of agency personnel with Training for Derivative Classifiers.

ISOO required agencies to indicate the percentage of personnel whose duties significantly involve the designation and/or handling of classified information that were rated on the designation and/or management of classified information. Only 35.6 percent of agencies reported this information. Of those that responded, 81.3 percent reported that 100 percent of their personnel are meeting this requirement; however, when including all agencies, and not only those that fulfilled ISOO's reporting requirement, only 28.9 percent reported that 100 percent of their personnel met this requirement.

In summary, ISOO will place special emphasis on assisting agencies to improve their CNSI posture through vigorous self-inspection programs, and to improve their reporting to ISOO on those programs. Self-inspection programs help decrease the likelihood of deficiencies, infractions and security violations, including instances of misclassification, improper safeguarding, unauthorized disclosures and untimely declassification. Agencies are more likely to have successful CNSI programs with the use of self-inspection programs.

Interagency Security Classification Appeals Panel

Mandatory Declassification Review Appeals

During FY 2012, the Panel continued to allocate a significant portion of its time and resources to processing MDR appeals. Appellants properly filed MDR appeals with the Panel in accordance with E.O. 13526 and the Panel's bylaws. In FY 2012, the Panel decided upon 35 MDR appeals, containing a total of 163 documents. The documents within these MDR appeals were classified either in part or in their entirety. The Panel declassified additional information in 150 documents (92 percent), and affirmed the prior agency classification decisions in 13 documents (8 percent). Of the 150 documents identified for additional declassification, the Panel declassified 63 documents (39 percent) in their entirety and 87 documents (53 percent) in part and affirmed the remaining classified portions.

Since May 1996, the Panel acted on a total of 1,358 documents. Of these, the Panel declassified additional information in 68 percent of the documents. Specifically, the Panel declassified 354 documents (27 percent) in their entirety and declassified 564 documents (41 percent) in part and affirmed the remaining classified portions. During this time frame, the Panel fully affirmed the classification decisions of agencies in 440 documents (32 percent).

Exemptions from Declassification

Section 3.3 (h) of the Order required significant revisions to agency exemptions to automatic declassification at the end of December 2012. Agencies made these revisions frequently in their declassification guides. In early 2011, the ISCAP Staff informed agency declassification offices of the need to identify specific information for exemption from automatic declassification at 25 years. Additionally, agencies needed to identify any extraordinary cases where information should be exempted from automatic declassification at 50 and 75 years. Agencies submitted their declassification guides to the Panel by December 31, 2011, and the Panel began the review, amendment, and approval process for 23 guides in January 2012. The Panel increased the frequency of its meetings to two per month and lengthened the duration of these meetings to five hours in order to fulfill its responsibilities to review declassification guides while still adjudicating MDR appeals. The Panel approved five guides in FY 2012 and the rest in FY 2013. ISOO published the results of the declassification guide approval process as an ISOO Notice listing those agencies eligible to exempt information at 25, 50, and 75 years.

ISCAP Decisions Web Site

In September 2012, the ISCAP Staff created a new web site displaying electronic versions of documents the Panel recently declassified for public use. Section 5.3(b)(4) of the Order requires that the Panel "appropriately inform senior agency officials and the public of final Panel decisions on appeals under sections 1.8 and 3.5 of this order." This requirement is important for two reasons. First, the Panel adjudicates classification challenges and mandatory declassification review appeals that may be of historical interest to the public, not just the appellants. Second, section 3.1(i) of the Order states that, "When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel." Distribution of electronic versions of declassified documents on a publicly available web site is the most efficient way for the Panel to provide senior agency officials and the public with its decisions and fulfill this requirement. The Panel will supplement and refine documents on the web site as the Panel and agencies declassify and release additional information.

Background

The President created the Panel by executive order in 1995 to perform the functions noted above. The Panel first met 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. ISOO provides staff support to Panel operations.

Authority

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

Functions

Section 5.3(b)

(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*

Mark A. Bradley, Acting Chair
Department of Justice

Margaret P. Grafeld
Department of State

Reginald D. Hyde
Department of Defense

Mary I. Ronan
National Security Staff

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.

**Note: The individuals named in this section were in these positions as of the end of FY 2012.*

Support Staff

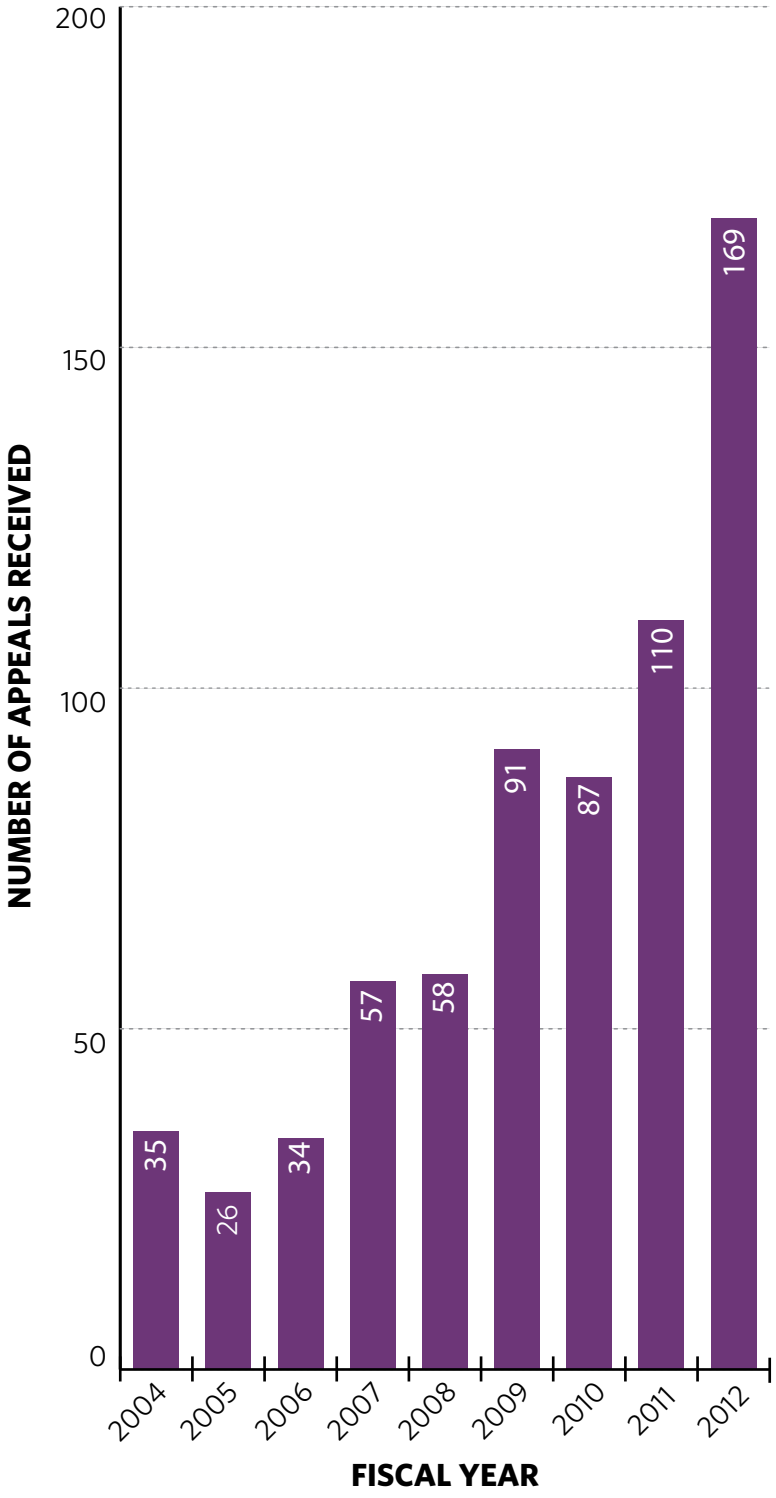
Information Security Oversight Office

For questions regarding the ISCAP, please contact the ISCAP's support staff:

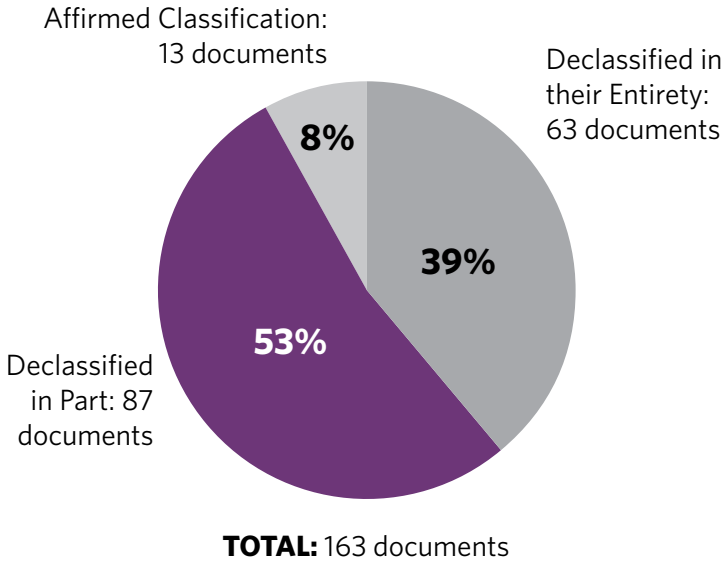
Telephone: 202.357.5250
Fax: 202.357.5908
E-mail: iscap@nara.gov

You can find additional information, including declassified and released documents, on the ISCAP website *http://www.archives.gov/declassification/iscap*

Number of Appeals Received by ISCAP

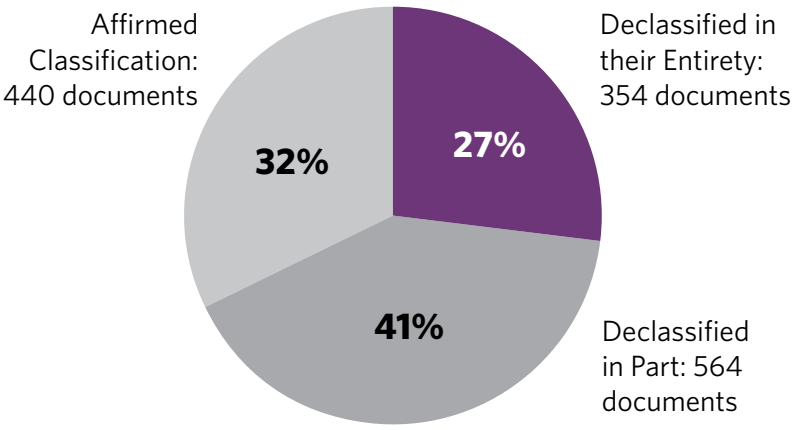


ISCAP Decisions, FY 2012



TOTAL: 163 documents

ISCAP Decisions, May 1996 – September 2012



TOTAL: 1,358 documents

The National Industrial Security Program

During FY 2012, the National Industrial Security Program Policy Advisory Committee (NISPPAC) held three meetings at the National Archives in Washington, D.C. Members discussed the timeliness of processing contractor personnel security clearances, the certification and accreditation of information systems processing classified information, status and plans for eliminating non GSA-approved security containers, special access programs, industry access to threat data, and the on-going revision of the National Industrial Security Program Operating Manual (NISPOM).

The Personnel Security Clearance (PCL) working group continued to review and analyze a comprehensive set of metrics that measure the timeliness of PCL processing for industry. This analysis includes metric data from the Office of Personnel Management, the Office of the Director of National Intelligence, the Department of Energy, the Department of Defense, and the Nuclear Regulatory Commission. The findings provide a comprehensive view of contractor clearance processes and issues, which resulted in numerous improvements such as upgrades to the e-QIP and electronic fingerprinting submittals. Likewise, the Certification and Accreditation (C&A) of information systems working group continued its review and analysis of the processes for approval of contractors, grantees and licensees of the Federal agencies to process classified information on designated systems. This group continued to recommend changes to policies and standards and tracked performance metrics to monitor the consistency, timeliness and effectiveness of the C&A processes.

In FY 2012, ISOO formed a new working group to support the implementation of NISP processes mandated in Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." This working group will ensure industry will fully integrate the mandatory structural reforms found in E.O. 13587 into NISP processes and implementation standards.

The NISPPAC continued to facilitate numerous review sessions of the NISPOM, the regulations governing protection of classified information in industry. Designated representatives of industry, the Cognizant Security Agencies, and other affected agencies reviewed and recommended revisions to existing guidelines and proposed changes to the NISPOM. As a result of this effort, the Defense Security Service, under DoD, anticipate the issuance of a conforming change to the current NISPOM in FY 2013 as well as a comprehensive update of the NISPOM in FY 2014.

The NISPPAC discussed the continued impact of the issuance of E.O. 13556, "Controlled Unclassified Information" (CUI), on the NISP contractors, grantees, or licensees. The inclusion of NISPPAC industry representatives in CUI implementation efforts will ensure its successful continuity and integration into NISP processes and implementation standards.

Finally, in FY 2012, the NISPPAC continued outreach and support to numerous industrial security entities, including the National Classification Management Society, Aerospace Industries Association-National Defense Intelligence Council, American Society for Industrial Security International, and Industrial Security Awareness Council.

Background

ISOO is responsible for implementing and overseeing the National Industrial Security Program (NISP) mandated under E.O. 12829, as amended, in 1993. ISOO executes this oversight responsibility primarily through the NISPPAC, a Federal Advisory Committee organized pursuant to section 103 of the NISP Executive Order. Both Government and industry representatives are members of the NISPPAC. The Department of Defense is the NISP executive agent and the Director of ISOO serves as the chair of the NISPPAC.

The NISPPAC advises on all matters involving the policies of the NISP and recommends 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 must convene at least twice a calendar year at the discretion of the ISOO Director or the Designated Federal Official for the NISPPAC. ISOO administers NISPPAC meetings in accordance with the Federal Advisory Committee Act. These meetings are open to the public.

The NISPPAC convenes several government/industry working groups to address action items and issues of mutual interest and concern. These permanent and ad-hoc working groups enhance the NISPPAC by gathering empirical data and developing process improvements to produce effective results for the program as a whole, reporting their findings at each NISPPAC meeting.

Authority

Executive Order 12829, as amended, "National Industrial Security Program"

Chairman

John P. Fitzpatrick, Director
Information Security Oversight Office

Support Staff

Information Security Oversight Office

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

Cost Estimates for Security Classification Activities

Background and Methodology

The Information Security Oversight Office (ISOO) reports annually to the President on the estimated costs associated with agencies' implementation of Executive Order (E.O.) 13526, "Classified National Security Information," and E.O. 12829, as amended, "National Industrial Security Program."

ISOO relies on the agencies to estimate and report the costs of the security classification system. The collection methodology used in this report has consistently provided a good indication of the trends in total cost. It is important to note that even if reporting agencies had no security classification activity, many of their reported expenditures would continue in order to address other, overlapping security requirements, such as work force, facility and information systems protection, mission assurance operations and similar needs.

The Government data presented in this report were collected by categories based on common definitions developed by an executive branch working group. The categories are defined below:

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

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

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 review programs established by E.O. 13526, as well as discretionary declassification activities and declassification activities required by statute.

Protection and Maintenance for Classified Information Systems: 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 computer hardware and software for protection of classified information, material, or processes in automated systems.

Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM)

OPSEC: Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

TSCM: Personnel and operating expenses associated with the development, training and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

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, Oversight, 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 specific or agency specific activities that are not reported in any of the primary categories, but are nonetheless significant and need to be included.

Results – Government Only

The total security classification cost estimate within Government for FY 2012 is $9.77 billion, a decrease of $1.59 billion, or 14 percent, from FY 2011. This figure represents estimates

provided by 42 executive branch agencies, including the Department of Defense (DoD). It does not include the cost estimates of the Central Intelligence Agency, the Defense Intelligence Agency, the Office of the Director of National Intelligence, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the National Security Agency. The cost estimates of these agencies are classified in accordance with Intelligence Community (IC) classification guidance and are included in a classified addendum to this report. If added in, the total costs of the IC agencies would add approximately 20% to the overall government total.

For FY 2012, agencies reported $1.38 billion in estimated costs associated with Personnel Security, a decrease of $25.25 million, or 2 percent.

Estimated costs associated with Physical Security were $1.69 billion, a decrease of $47.47 million, or 3 percent.

Estimated costs associated with Classification Management were $327.92 million, a decrease of $24.47 million, or 7 percent.

Estimated costs associated with Declassification were $48.65 million, a decrease of $4.11 million, or 8 percent.

Estimated costs associated with Protection and Maintenance for Classified Information Systems were $4.03 billion, a decrease of $1.61 billion, or 29 percent. The majority of this decrease is due to agencies improving their ability to distinguish systems security costs for classified systems from those of their unclassified systems. Only costs for classified systems are to be reported to ISOO.

Estimated costs associated with OPSEC and TSCM were $124.46 million, a decrease of $4.51 million, or 3 percent.

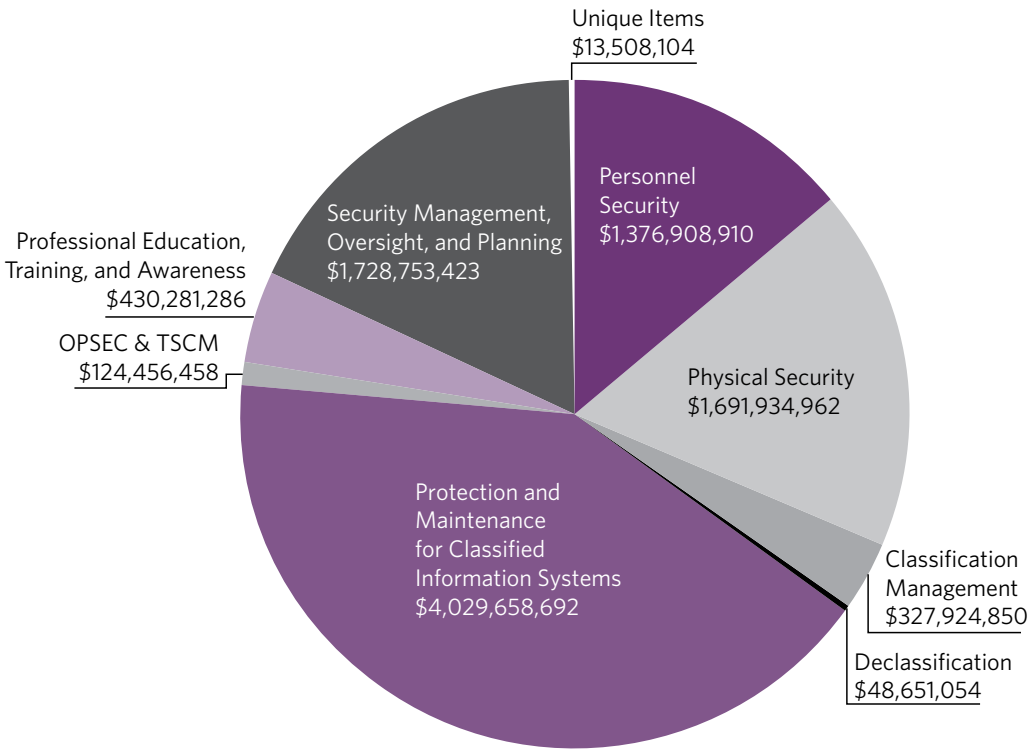
Together, costs for Classification Management, Declassification, Protection and Maintenance for Classified Information Systems, and OPSEC and TSCM make up the total cost for Information Security which is $4.53 billion, a decrease of $1.65 billion, or 27 percent.

The FY 2012 estimated costs for Professional Education, Training, and Awareness were $430.28 million, a decrease of $72.23 million, or 14 percent. Agencies are attending fewer training conferences and are increasing use of web-based training.

Estimated costs associated with Security Management, Oversight, and Planning were $1.73 billion, an increase of $201.04 million, or 13 percent. This increase is due to additional funding required to conduct compliance surveys, assessments, inspections, and accreditation of classified systems.

Estimated costs associated with Unique Items were $13.51 million, an increase of $1.60 million, or 13 percent.

Government Security Classification Costs FY 2012



TOTAL: $9,772,077,739

*Government Security Classification Costs FY 1995–FY 2012**

	Personnel Security	Physical Security	Classification Management	Declassification*	Protection & Maintenance for Classified Information Systems	OPSEC & TSCM+	Professional Education, Training, & Awareness	Security Management, Oversight, & Planning	Unique Items	TOTAL
1995	$633 million	$175 million	$312 million	—	$1.2 billion	—	$67 million	$257 million	$6.4 million	$2.7 billion
1996	$479 million	$308 million	$325 million	—	$1.2 billion	—	$72 million	$343 million	$5.6 million	$2.7 billion
1997	$390 million	$345 million	$429 million	—	$1.79 billion	—	$78 million	$399 million	$4.2 million	$3.4 billion
1998	$398 million	$386 million	$212.96 million	$199.65 million	$1.82 billion	—	$93 million	$487 million	$5.7 million	$3.6 billion
1999	$426 million	$410 million	$219 million	$233.18 million	$1.91 billion	—	$97 million	$480 million	$0. 8 million	$3.77 billion
2000	$426 million	$272 million	$212.75 million	$230.90 million	$2.55 billion	—	$112 million	$439 million	$25 million	$4.27 billion
2001	$859 million	$217 million	$221.30 million	$231.88 million	$2.50 billion	—	$106 million	$539 million	$25 million	$4.7 billion
2002	$941 million	$367 million	$236.97 million	$112.96 million	$3.12 billion	—	$134 million	$742 million	$26 million	$5.68 billion
2003	$950 million	$536 million	$264.66 million	$53.77 million	$3.66 billion	$15.01 million	$158 million	$858 million	$27.7 million	$6.52 billion
2004	$941 million	$691 million	$323.87 million	$48.26 million	$3.90 billion	$12.22 million	$178 million	$1.15 billion	$6.4 million	$7.25 billion
2005	$1.15 billion	$1.04 billion	$309.93 million	$56.83 million	$3.64 billion	$33.64 million	$219 million	$1.21 billion	$6.6 million	$7.66 billion
2006	$1.11 billion	$1.06 billion	$312.90 million	$43.99 million	$4.02 billion	$88.42 million	$237 million	$1.36 billion	$7.3 million	$8.24 billion
2007	$1.10 billion	$1.37 billion	$323.50 million	$44.59 million	$4.18 billion	$85.57 million	$211 million	$1.33 billion	$7.9 million	$8.65 billion
2008	$1.10 billion	$1.29 billion	$333.71 million	$42.73 million	$4.34 billion	$90.15 million	$243 million	$1.20 billion	$8.8 million	$8.65 billion
2009	$1.21 billion	$1.28 billion	$361.17 million	$44.65 million	$4.26 billion	$106.14 million	$226 million	$1.30 billion	$15.7 million	$8.80 billion
2010	$1.56 billion	$1.43 billion	$364.22 million	$50.44 million	$4.69 billion	$106.65 million	$400 million	$ 1.54 billion	$21.9 million	$10.16 billion
2011	$1.40 billion	$1.74 billion	$352.40 million	$52.76 million	$5.65 billion	$128.97 million	$502.51 million	$1.53 billion	$11.9 million	$11.36 billion
2012	$1.38 billion	$1.69 billion	$327.92 million	$48.65 million	$4.03 billion	$124.46 million	$430.28 million	$1.73 billion	$13.51 million	$9.77 billion

*Prior to 1998, Declassification costs were included in Classification Management costs.
+Prior to 2003, OPSEC and TSCM costs were not reported.

Results – Industry Only

To fulfill the cost reporting requirements, a joint DoD and industry group developed a cost collection methodology for those costs associated with the use and protection of classified information within industry. For FY 2012, the Defense Security Service collected industry cost data and provided the estimate to ISOO.

Cost estimate data are not provided by category because industry accounts for its costs differently than Government. Rather, a sampling method was applied that included volunteer companies from four different categories of facilities.

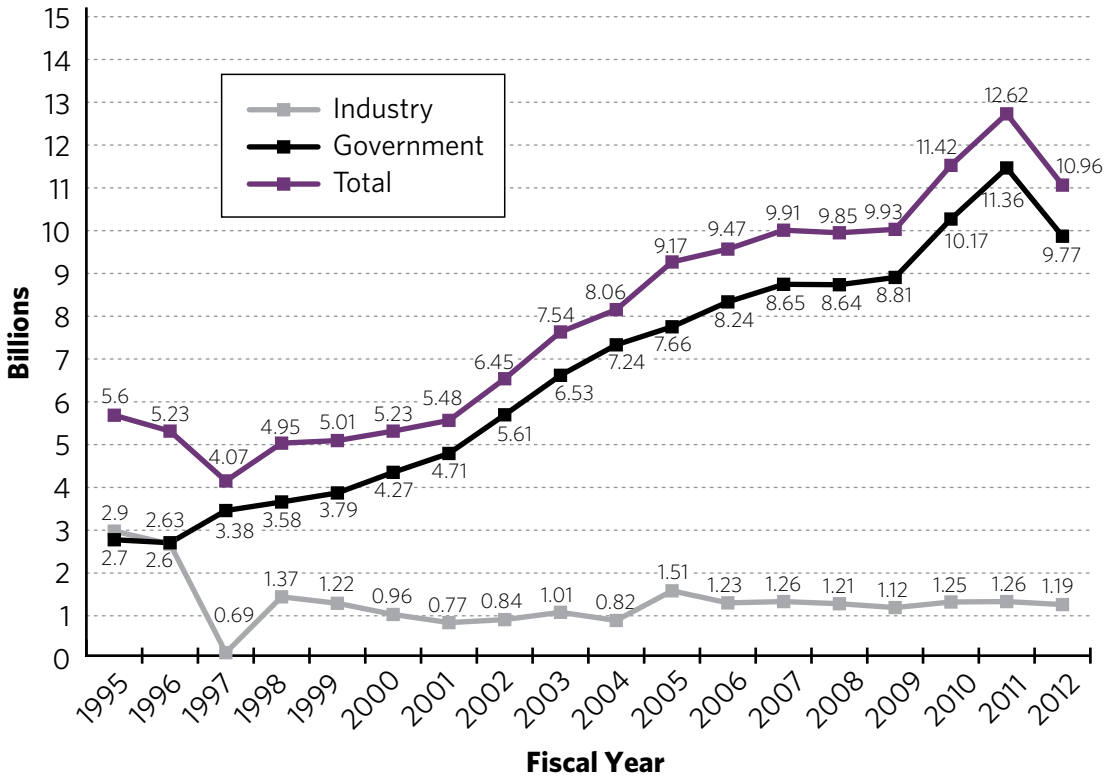
The category of facility is based on the complexity of security requirements that a particular company must meet in order to hold and perform under a classified contract with a Government agency.

The FY 2012 cost estimate totals for industry pertain to the twelve-month accounting period for the most recently completed fiscal year of the companies that were part of the industry sample under the National Industrial Security Program. The estimate of total security classification costs for FY 2012 within industry is $1.19 billion; a decrease of $67.72 million, or 5 percent.

Results – Combined Government and Industry

This year's combined estimate for Government and industry was $10.96 billion, a decrease of $1.66 billion, or 13 percent.

Total Costs for Government and Industry FY 1995 – FY 2012



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