NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

ISOO

INFORMATION SECURITY
OVERSIGHT OFFICE

2013

# *Report to the President*

# 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. 13556, "Controlled Unclassified Information"
- 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.
- Serve as Executive Agent to implement E.O. 13556 and oversee agency actions.
- 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 programs for protection of classified and controlled unclassified information.
- Reduce classification and control activity to the minimum necessary.
- Ensure that the systems for declassification and decontrol operate as required.
- Provide expert advice and guidance to constituents.
- Collect, analyze, and report valid information about the status of agency programs.

# Letter to the President

June 2, 2014

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 2013, 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. It also contains the status of agency self-assessment reporting, the cost of security classification activity, and the National Industrial Security Program.

I have also incorporated the required annual report on the development of the Controlled Unclassified Information program into this report. ISOO fulfills Executive Agent (EA) responsibilities for the Controlled Unclassified Information (CUI) Program, which were designated by Executive Order 13556 to the National Archives and Records Administration. During the past year, as EA, ISOO successfully advanced its policy development strategy, worked with the Office of Management and Budget to issue guidance for the Executive branch on submission of information types as CUI categories, established a CUI Advisory Council to improve consultative functions, and is currently completing a draft implementing directive. When the directive is incorporated into the Code of Federal Regulations, the EA plans to issue a National Implementation Plan for the Executive branch, providing a timeline detailing phases of implementation for all agencies.

With regard to its oversight of Classified National Security Information, ISOO continues to develop and refine its ability to monitor agency efforts to perform self-assessment of their classified information programs. The agency self-inspection reports were much more responsive in this, the third year of detailed reporting required by E.O. 13526. This improvement is due, in large part, to the use of a new reporting form. Further improvement is needed in the quality of the reports from some agencies. ISOO will continue to use the self-inspection reporting process and its on-site assessment authority to prompt agencies to evaluate and improve their classified national security information programs.

The Interagency Security Classification Appeals Panel continued adjudicating declassification appeals and posting the decisions on a publicly available website. The growing collection of over 250 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 also helps agencies to 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. 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. ISOO continues its role on the Senior Information Sharing and Safeguarding Steering Committee, leading efforts to incorporate the requirements of the National Insider Threat Policy, and related responses to unauthorized disclosures, into the National Industrial Security Program policy and guidance.

Lastly, ISOO joined with its Federal security partners as a member of the Office of Management and Budget-led Suitability and Security Processes Review, which made recommendations critical to the efforts to reform security clearance and related processes. Not only did this leverage ISOO's long history of involvement in these matters and its role in overseeing and ensuring the viability and accountability of cleared contractors in the clearance process, but it dovetailed with my own experience leading related efforts at clearance reform in the Executive branch. ISOO is poised to continue its support to these and future reforms.

Respectfully,

John P. Fitzpatrick

JOHN P. FITZPATRICK
Director

# Table of Contents

# *Summary of FY 2013 Program Activity*

## Classification

Executive branch agencies reported 2,269 original classification authorities (OCA), down from 2,326 reported in FY 2012.

Agencies reported 58,794 original classification decisions, a decrease of 20 percent.

Agencies reported using the ten-years-or-less declassification instruction for 61 percent of original classification decisions.

Executive branch agencies reported 80,124,389 derivative classification decisions; a 16 percent decrease from FY 2012.

## Declassification

Agencies received 9,521 initial mandatory declassification review (MDR) requests and closed 6,477 requests. The average number of days to resolve each request is 175. A total of 8,749 requests have remained unresolved for over one year. This number includes requests that have been carried over from prior years.

Agencies reviewed 1,122,502 pages under MDR, and declassified 943,035 pages in their entirety, declassified 150,857 pages in part, and retained classification of 28,610 pages in their entirety.

Agencies received 440 MDR appeals and closed 311 appeals. The average number of days to resolve each appeal is 186. A total of 326 appeals have remained unresolved for over one year.

Agencies reviewed 33,390 pages on appeal, and declassified 26,243 pages in their entirety, declassified 4,483 pages in part, and retained classification of 2,664 pages in their entirety.

Under automatic declassification, agencies reviewed 52,470,623 pages and declassified 25,771,199 pages of historically valuable records.

Under systematic declassification reviews, agencies reviewed 6,515,055 pages, and declassified 1,697,472 pages.

Under discretionary declassification reviews, agencies reviewed 346,351 pages, and declassified 55,671 pages.

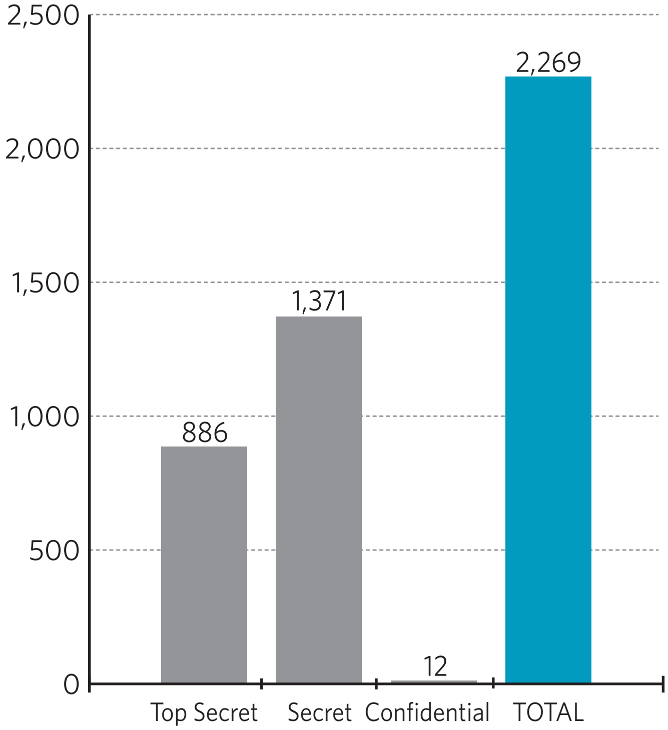
Under automatic, systematic, and discretionary declassification reviews, a total of 59,332,029 pages were reviewed for declassification and 27,524,342 pages were declassified.

# *Classification*

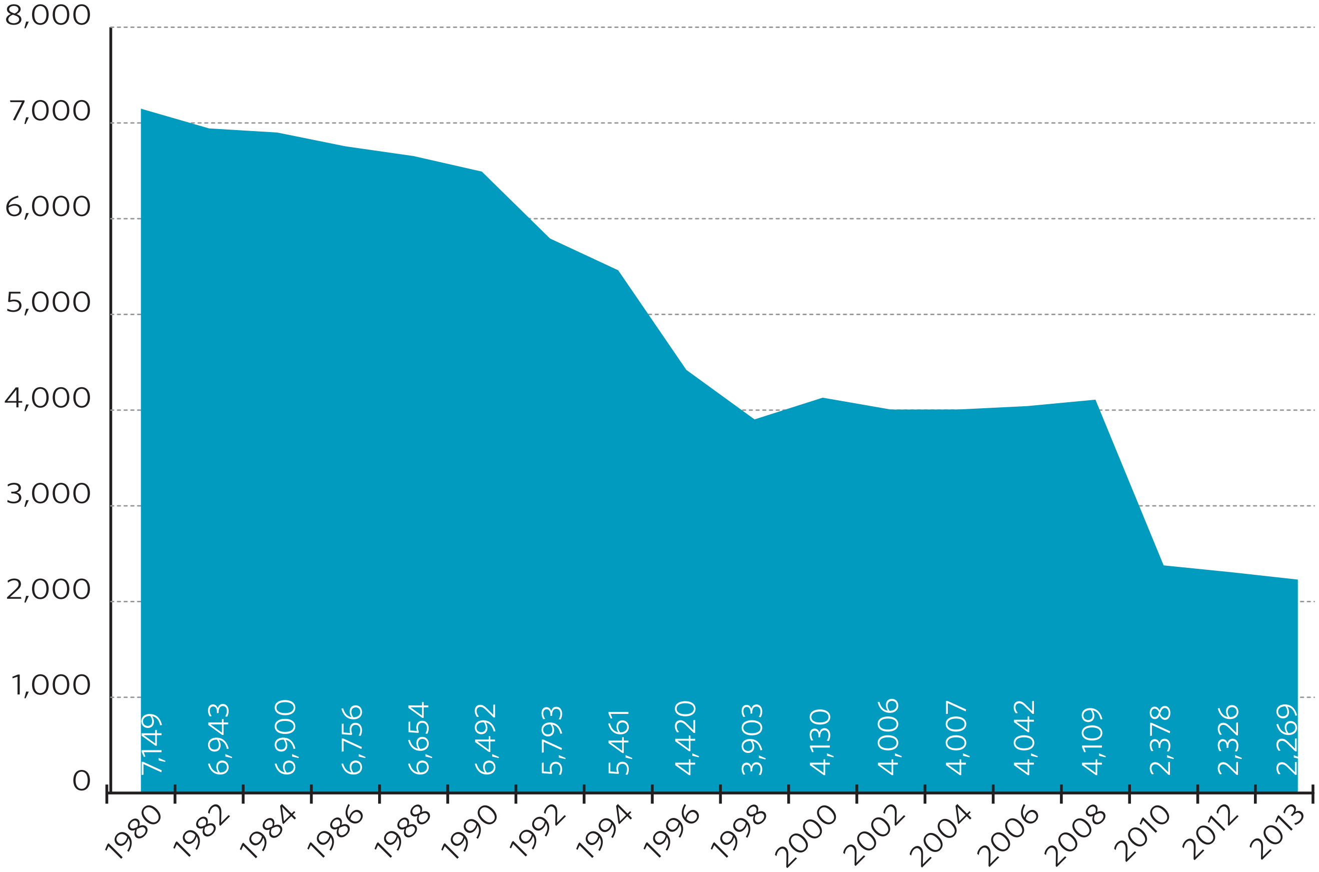
## Original Classification Authorities

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 2,269 OCAs in FY 2013; a 2 percent decrease from the 2,326 reported in FY 2012.

Original Classification Authorities, FY 2013



Number of Original Classification Authorities, FY 1980 - FY 2013



*By definition, original classification precedes all other aspects of the security classification system, including derivative classification, safeguarding, and declassification.*

## Original Classification

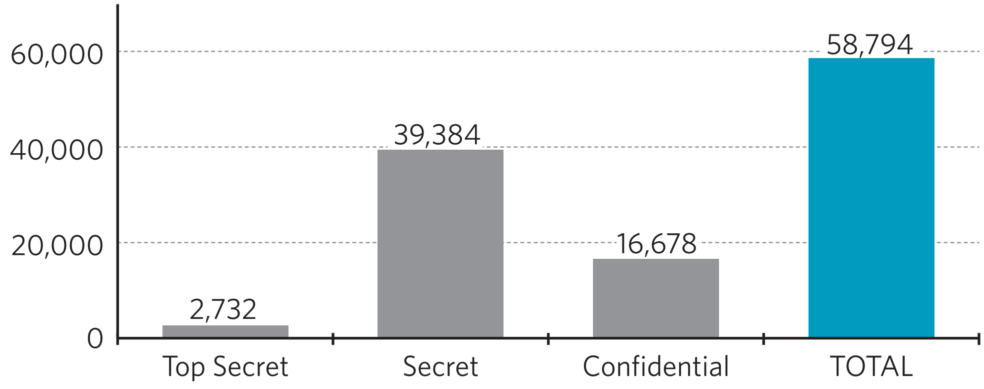
Original classification is a determination by an OCA that information owned by, produced by or for, or under the control of the U.S. Government requires protection because unauthorized disclosure of that information could reasonably be expected to cause damage to the national security.

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.

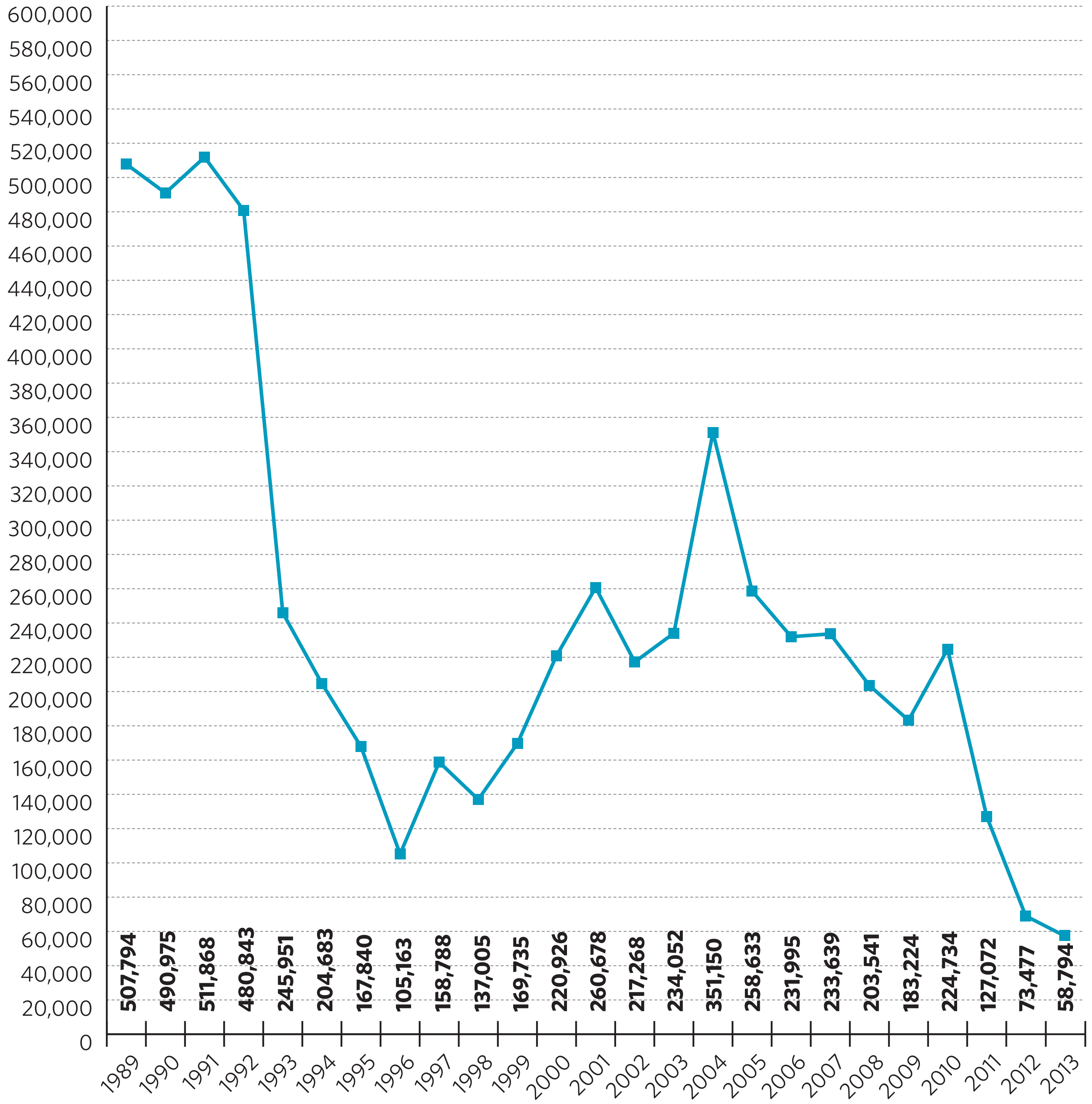
The agencies reported 58,794 original classification decisions for FY 2013, using the ten-year-or-less declassification instruction 61 percent of the time.

The agencies also reported a decrease of original classification decisions by 20 percent during FY 2013.

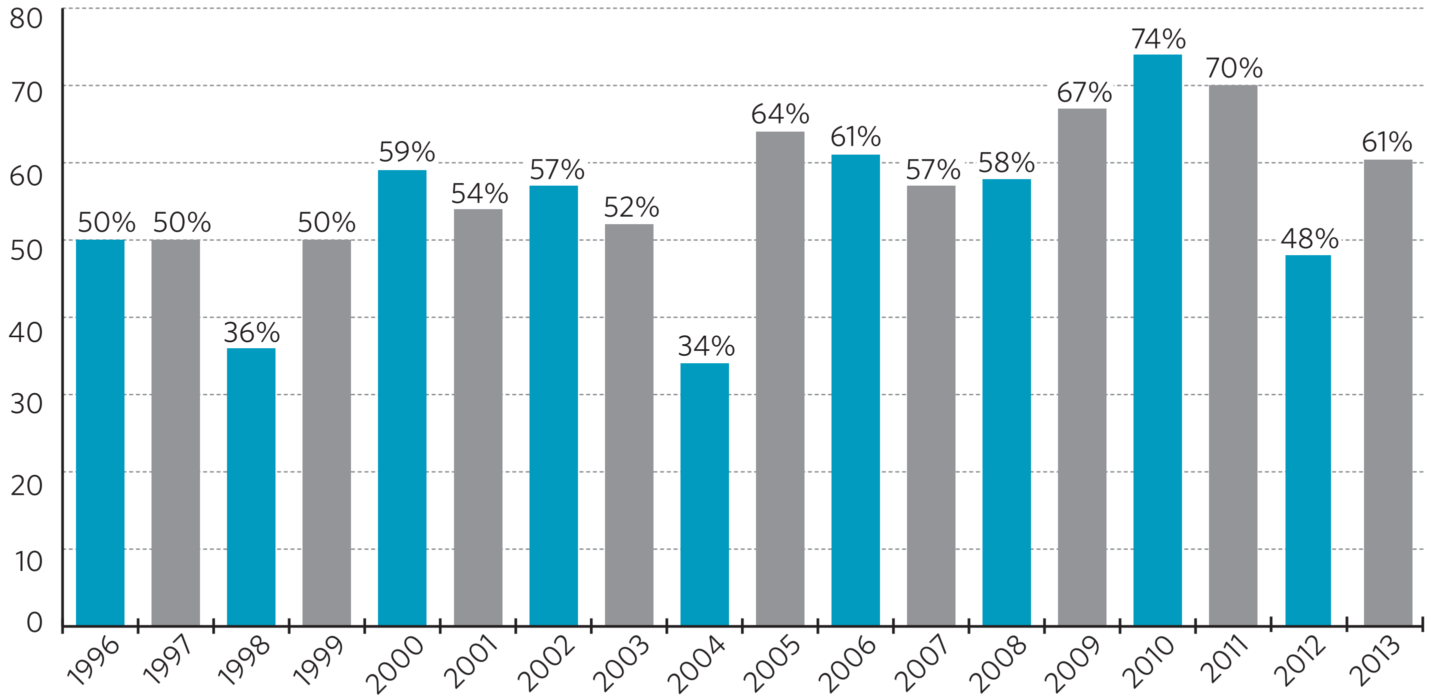
### Original Classification Activity, FY 2013



## Original Classification Activity, FY 1989 - FY 2013



## Use of the "Ten Years or Less" Declassification Category, FY 1996 - FY 2013



## 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. Classification guides provide consistency and accuracy to classification decisions.

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.

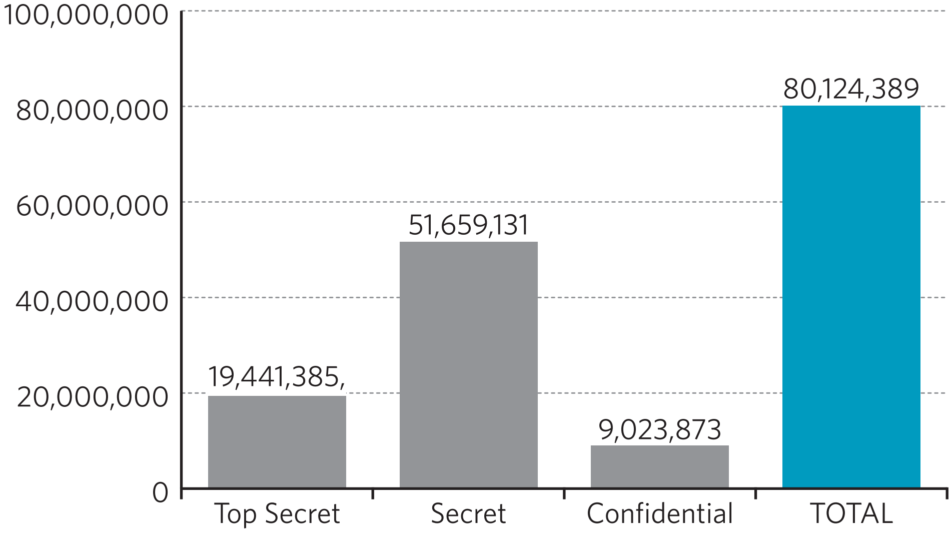
Agencies reported a total of 80.12 million derivative classification decisions in FY 2013, a decrease of 16 percent from FY 2012. Although we can not pinpoint a single cause for this decrease, we do know it was due in part to the refinement and correction of estimation practices employed by some agencies. Other possible contributing factors could be the recent emphasis on proper classification procedures coming from the expanded agency self-inspection requirements, the inspector-general reviews conducted in response to the Reducing Over-Classification Act, and the Fundamental Classification Guidance Reviews that all agencies conducted in 2012.

## Classification Challenges

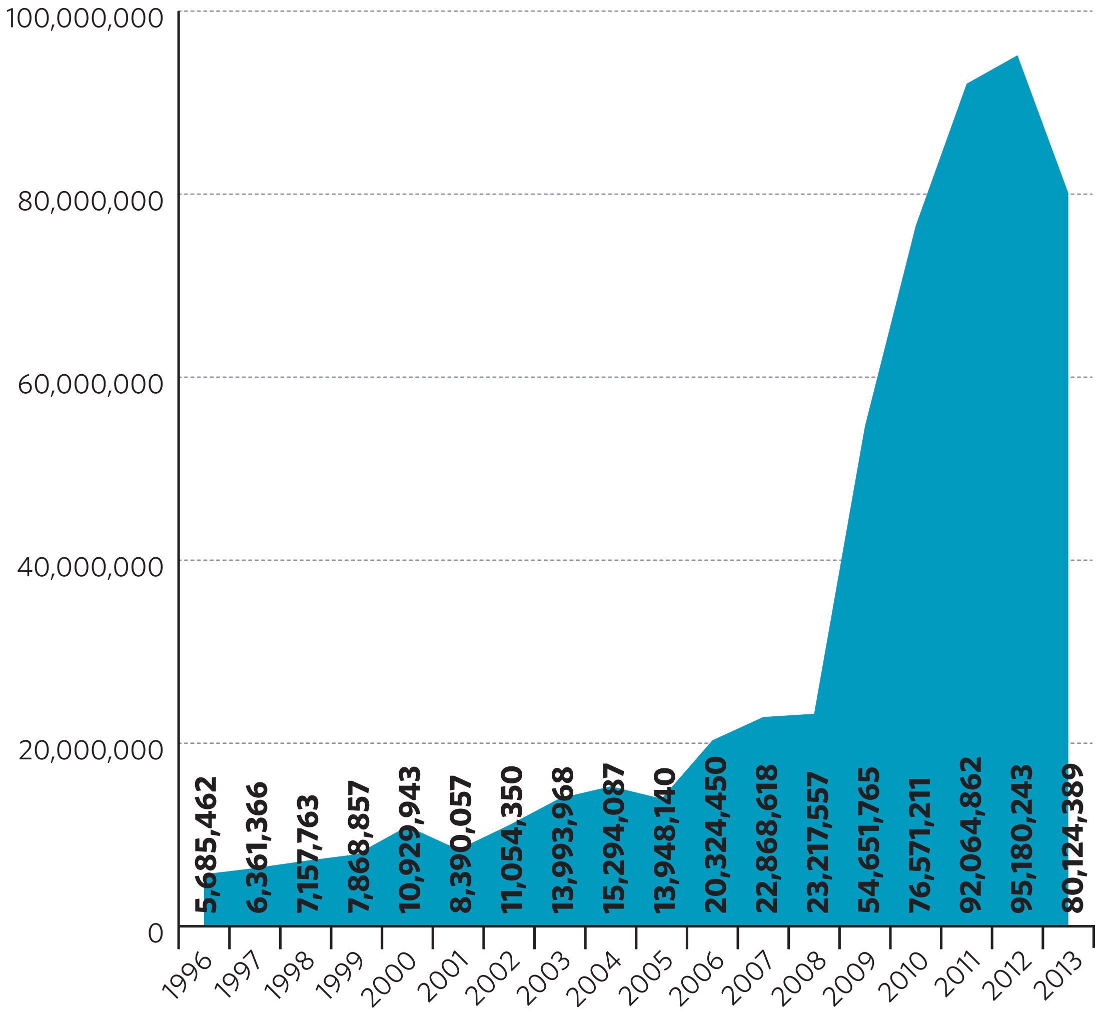
Authorized holders of information who, in good faith, believe its classification status is improper are encouraged and expected to challenge the classification status of that information. Classification challenges are handled both informally and formally, and provide individual holders the responsibility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

Agencies reported 68 formal challenges in FY 2013; 41 (60.3 percent) were fully affirmed at their current classification status with 12 (17.6 percent) being overturned either in whole or in part. Fifteen challenges remain open.

## Derivative Classification Activity, FY 2013



## Derivative Classification Activity, FY 1996 - FY 2013



# 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.

## Automatic, Systematic, and Discretionary Declassification Review

During FY 2013, a total of 59.33 million pages were reviewed under the automatic, systematic, and discretionary declassification programs and 27.52 million pages (46 percent) were declassified*. This is a 2 percent increase in the scale of declassification from FY 2012, when 44.92 million pages were reviewed and 19.85 million pages (44 percent) were declassified. While the percentage of pages declassified is just a small increase, the number of pages reviewed increased by over 14 million, while the number of pages declassified increased by almost 8 million over last year.

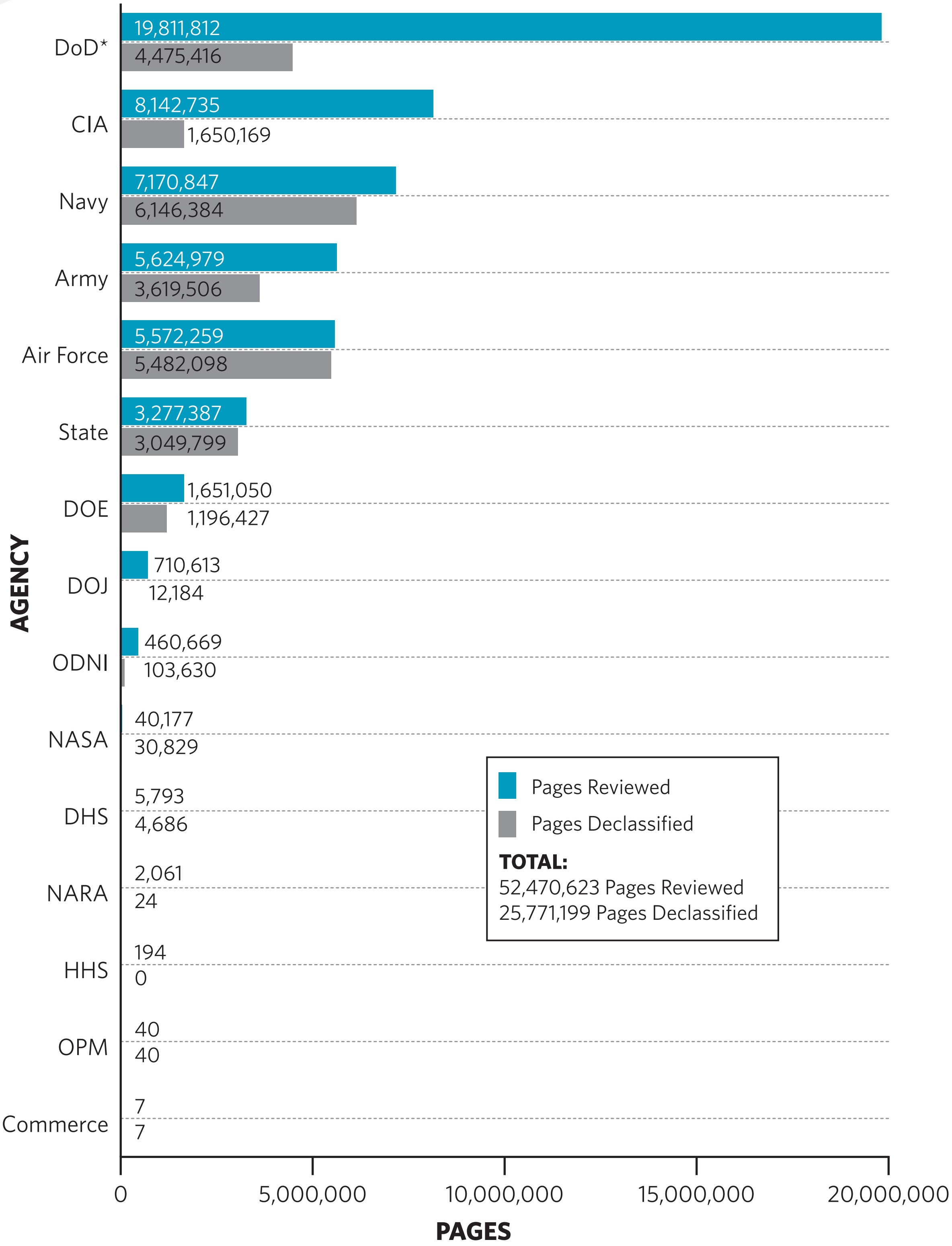
Under automatic declassification review, agencies reviewed 52.47 million pages and declassified 25.77 million pages (49 percent). Under systematic declassification review, agencies reviewed 6.52 million pages and declassified 1.70 million pages (26 percent). Under discretionary declassification review, agencies reviewed 346,351 pages and declassified 55,671 pages (16 percent).

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 documents processed by the National Declassification Center. Information about that program can be found at* ***http://www.archives.gov/declassification/ndc/releases.html***

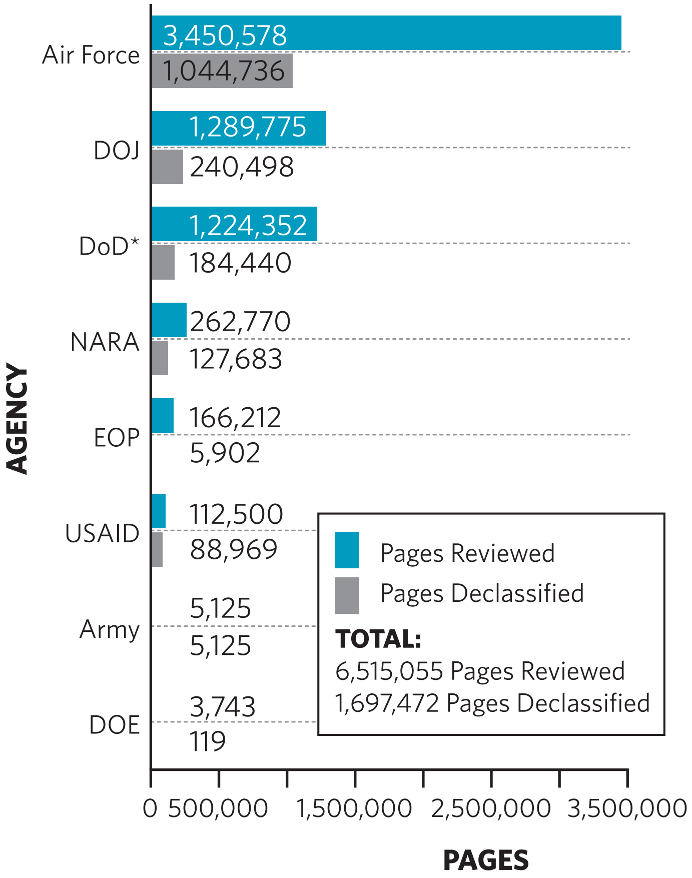
*During FY 2013, a total of 59.33 million pages were reviewed under the automatic, systematic, and discretionary declassification programs and 27.52 million pages (46 percent) were declassified.*

## Number of Pages Reviewed and Declassified for Automatic Declassification, FY 2013



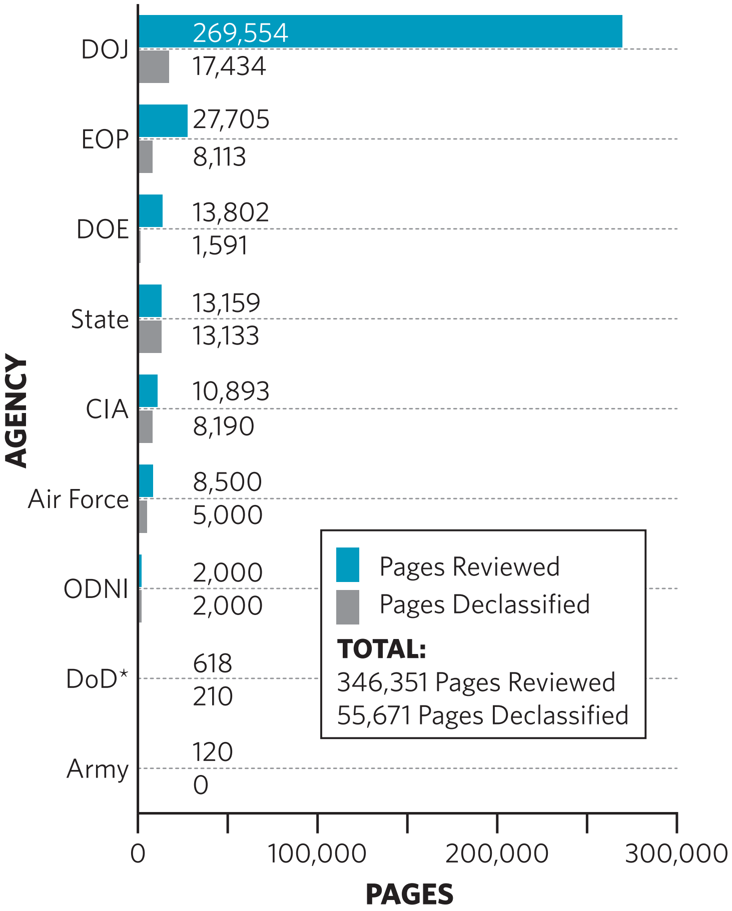
** DoD numbers do not include Air Force, Army, and Navy.*

## Number of Pages Reviewed and Declassified for **Systematic Declassification**, FY 2013



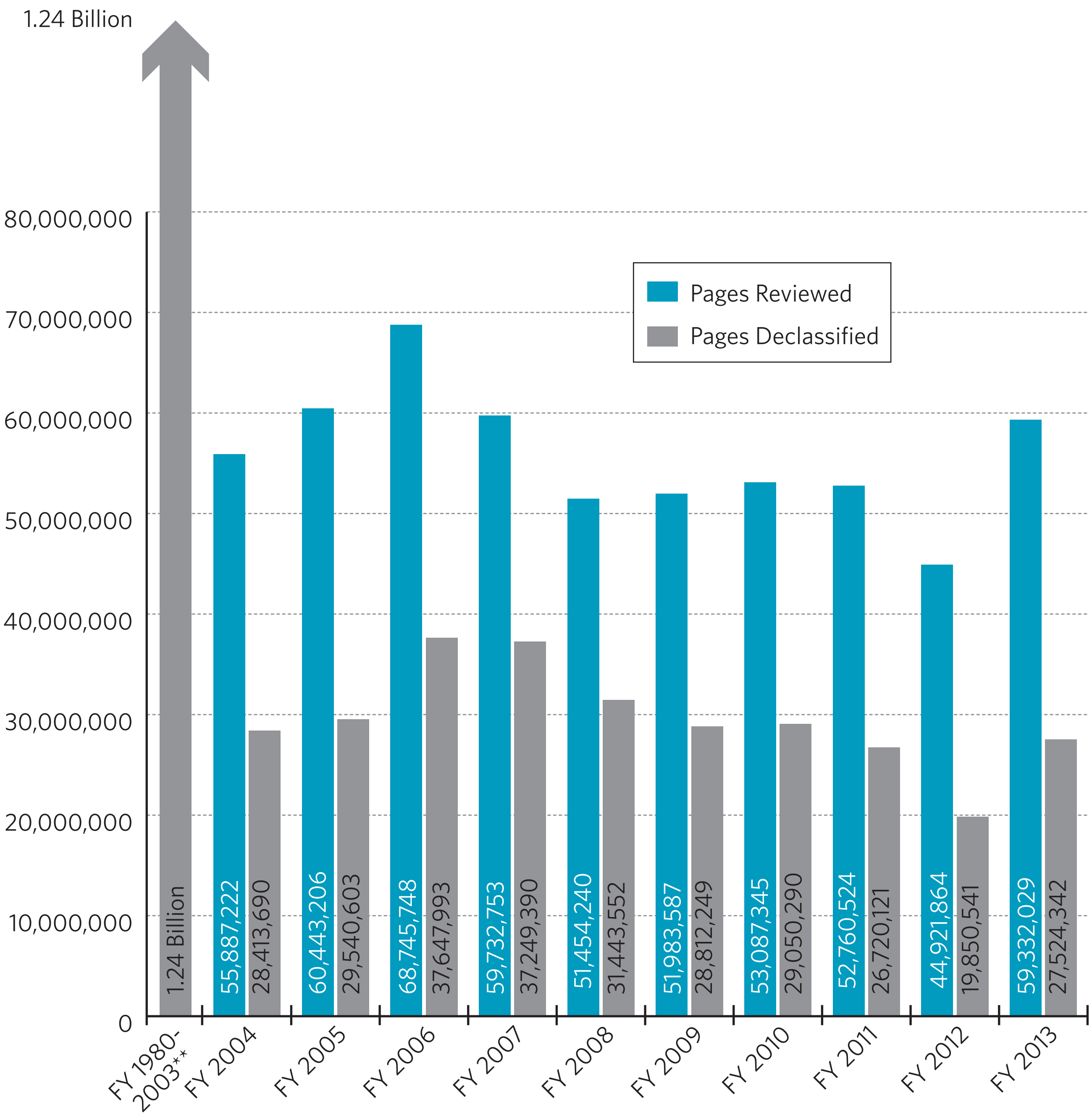
** DoD numbers do not include Air Force, Army, and Navy.*

## Number of Pages Reviewed and Declassified for **Discretionary Declassification**, FY 2013



** DoD numbers do not include Air Force, Army, and Navy.*

## Total Number of Pages Reviewed and Declassified*, FY 1980 - FY 2013 (Automatic, Systematic, and Discretionary Declassification Reviews)



** Excludes 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 2013

The FY 2013 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. The report also 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.

During FY 2013, there was a substantial increase in the number of pages reviewed for both MDR requests and appeals. Last year, there were 372,354 pages reviewed in 7,589 requests. This year, there were a total of 1,122,502 pages reviewed in the 9,521 requests received; an increase of 1,932 in requests received and an increase of 750,148 in pages reviewed. The percentage of pages declassified in their entirety also continues to increase from 58.4 percent in FY 2012 to 84 percent in FY 2013. This in no way indicates that the original classification decisions were incorrect; just that as times change, so does the sensitivity of the information. The fact that a higher percentage of pages are being declassified shows the careful consideration agency personnel are giving to the documents being reviewed. The percentage of pages denied declassification decreased from 18.3 percent in FY 2012 to just 3 percent in FY 2013.

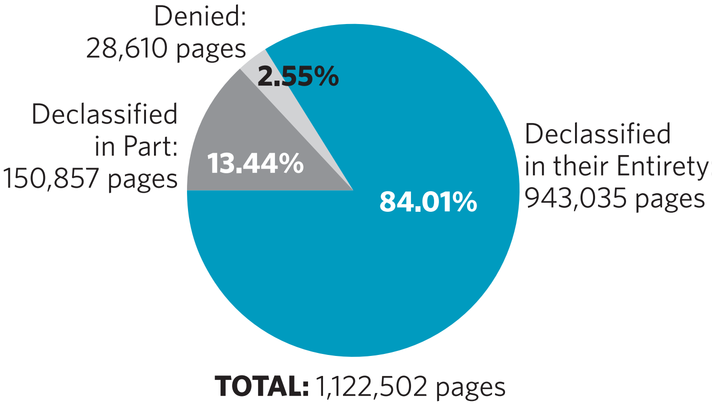
There was also an increase in the numbers of MDR appeals, 10,920 pages in 368 appeals in FY 2012 compared to 33,390 pages in 440 appeals in FY 2013. The percentage of pages declassified on appeal increased from 29.1 percent last year to 79 percent this year. The percentage of pages denied declassification decreased from 39.4 percent in FY 2012 to just 8 percent in FY 2013.

### Mandatory Declassification Review Program Activity, FY 2012 – FY 2013

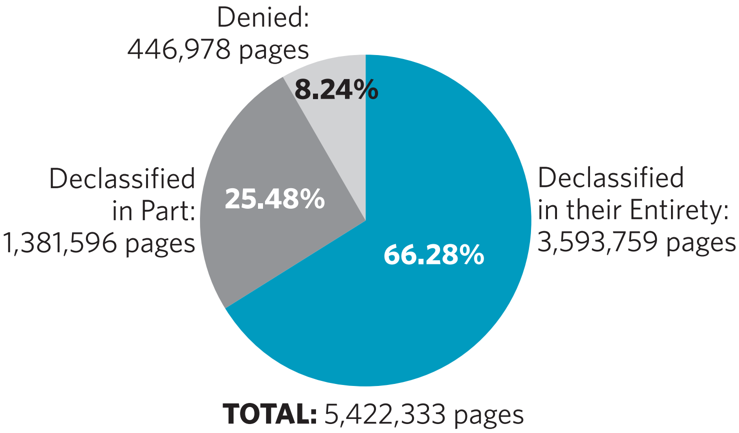
| **Requests** | **2012** | **2013** |
|---|---|---|
| Requests Received | 7,589 | 9,521 |
| Requests Closed | 6,533 | 6,477 |
| Requests Unresolved for Over One Year | 6,666 | 8,749 |
| Average Number Days to Resolve Each Request | 228 | 175 |
| **Appeals** | **2012** | **2013** |
| Appeals Received | 368 | 440 |
| Appeals Closed | 321 | 311 |
| Appeals Unresolved for Over One Year | 233 | 326 |
| Average Number Days to Resolve Each Appeal | 240 | 186 |
| **Referred** | **2012** | **2013** |
| Referred Requests Received* | 10,001 | 12,051 |
| Referred Appeals Received* | 212 | 211 |

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

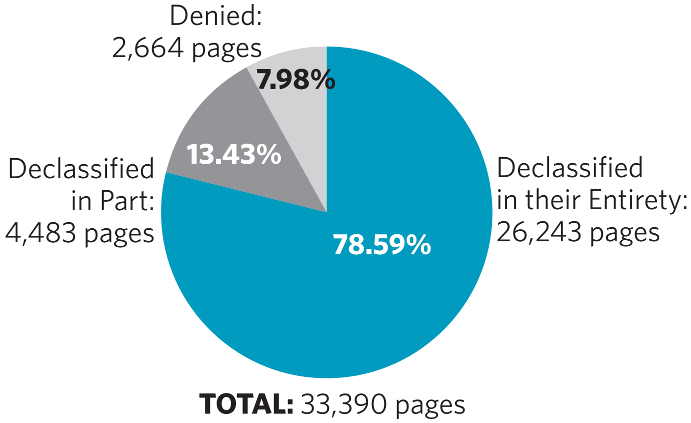
## Disposition of MDR Requests, FY 2013



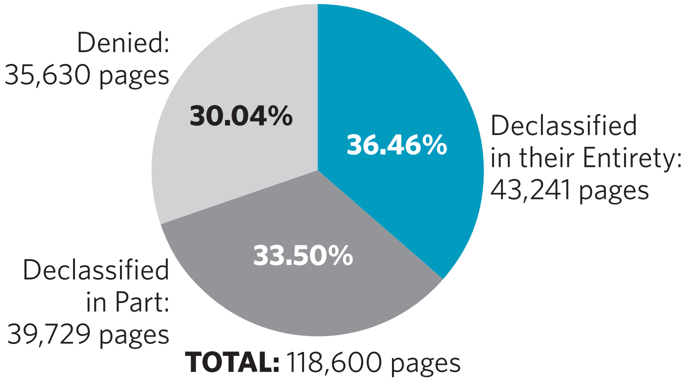
## Disposition of MDR Requests FY 1996 – FY 2013



## Disposition of MDR Appeals, FY 2013



## Disposition of MDR Appeals FY 1996 - FY 2013



# Reviews

## Declassification Assessments

In FY 2013, ISOO conducted declassification proficiency assessments of five agencies using an updated assessment plan and a revised scoring methodology. ISOO concluded its initial five-year assessment period in FY 2012 and accomplished its strategic goal of improving the quality of agency automatic declassification review programs.

Starting in FY 2013, ISOO modified its declassification assessment program to monitor agencies' steady-state performance. Under this approach, ISOO will monitor agency automatic declassification review programs and ensure that they maintain "high scores." ISOO designed the updated program to balance use of ISOO and agency resources with the need to monitor agency automatic declassification review proficiency. Before implementing changes to this program, ISOO met with officials from the National Declassification Center and agencies and conducted a detailed survey with stakeholders, asking for input into changes to improve the program.

The revised approach includes significant changes based on feedback from agencies and stakeholders. These changes include the establishment of a four-year review cycle, the revision of the assessment criteria and scoring tool, and the shift from a three-tiered scoring system to a two-tiered system. ISOO also changed its policy from bi-annual data requests to a single annual request and ISOO will base any on-site assessment on records the agency reviewed in the previous 12 months.

On an annual basis, ISOO will assess *at least 25 percent* of agencies reporting that they reviewed a significant volume of records for automatic declassification. Beginning in FY 2013, ISOO will assess agencies identified as having a significant automatic declassification review program at least once during the four-year period.

In this revised approach, ISOO issues a data request each February, asking agencies to provide information on records reviewed for automatic declassification between April 1 of the previous year and March 31 of the current year. It allows agencies to compile data and respond by the middle of May. After evaluating the responses, ISOO selects five or six agencies and conducts assessments of their programs.

ISOO also revised the scoring criteria for FY 2013-2016 to reflect stakeholder input and results from the assessments themselves. ISOO still focuses the assessments on three major areas of concern—missed equities, improper exemptions, and improper referrals.

» Missed equities indicate instances of a declassification review not identifying for referral the security classification interest of one agency found in the record of another agency;

» Improper exemptions indicate instances of a declassification review resulting in the attempt to exempt a record from automatic declassification under an exemption category not permitted by that agency's declassification guide as approved by the Interagency Security Classification Appeals Panel;

» Improper referrals indicate instances of a declassification review resulting in the referral of records to agencies lacking the authority to exempt information from declassification or waiving their interest in declassification.

ISOO declassification assessments factored the occurrence and extent of any of these three issues into the overall agency score for the assessment. In addition to these three main categories, ISOO also examined records to observe the extent that agency declassification policies are in compliance with ISOO regulations and are in place to best assist the National Declassification Center when it processes the records for public access. These policies include the full and appropriate use of the Standard Form (SF) 715, "Declassification Review Tab;" the appropriate age of the records reviewed (between 20-25 years of age); the use of box summary sheets; the use of appropriate record-keeping practices, including documenting completion of Kyl-Lott reviews; and the absence of unexplained multiple declassification reviews.

ISOO conducted on-site assessments of five agencies in FY 2013: the Federal Bureau of Investigation, the Joint Staff, the National Archives and Records Administration, the Department of State, and the U.S. Agency for International Development. All five agencies scored "high." While agencies improved the quality of agency automatic declassification reviews since FY 2008 when ISOO began this oversight program, ISOO continues to identify isolated instances of missed equities and improper referrals. In FY 2013, ISOO documented three instances of missed equities and two instances of improper referrals. Additionally, ISOO continues to note positive progress in policy and program implementation. In FY 2013, ISOO found that all agencies used box summary sheets and had effective record-keeping practices to document their review decisions. ISOO noted that, with only a single exception, agencies fully and appropriately used the SF 715. These practices facilitate the processing of referrals at the National Declassification Center.

In FY 2014, ISOO will continue to conduct annual declassification assessments of at least five agencies. It will continue to provide agency-specific training and issue notices to agencies in order to provide specific guidance on areas of concern.

### Declassification Assessment Results, FY 2013

| Agency | Result |
|---|---|
| Federal Bureau of Investigation | 100 |
| Department of State | 90 |
| National Archives and Records Administration | 90 |
| U.S. Agency for International Development | 90 |
| Joint Staff | 85 |

### Declassification Assessment Results, FY 2008 – FY 2013

| Fiscal Year | Number of Agencies | Average Score |
|---|---|---|
| 2008 | 22 | 79 |
| 2009 | 19 | 84 |
| 2010 | 15 | 90 |
| 2011 | 15 | 94 |
| 2012 | 16 | 97 |
| 2013 | 5 | 91 |

## Self-Inspections

E.O. 13526 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.

In order for senior agency officials (SAO) to fulfill their responsibilities under E.O. 13526, agency self-inspection programs must be structured to provide the SAOs information to assess the effectiveness of each agency's classified national security information (CNSI) program. Effective self-inspection programs generally correlate to effective 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.

The implementing directive for E.O. 13526, 32 CFR Part 2001, requires that 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 a summary and assessment 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. To ensure that agencies cover key requirements of the Order, the reports must also answer questions relating to areas such as training, performance evaluations, and classification challenges.

In the first two years of descriptive self-inspection reporting required under E.O. 13526, a large percentage of the agencies submitted reports that failed to cover many of the required elements. In 2012, only about 10 percent provided responses addressing all or nearly all of the required areas. In an effort to improve upon this, ISOO created a self-inspection reporting form and required agencies to submit their responses on it. In 2013, using the new form, nearly 80 percent of the agencies submitted reports that covered all or nearly all of the required areas. The greatest improvement in responsiveness was to the questions relating to key requirements of the Order and in providing data from the review of classification actions. While further improvement in the quality of reports is needed at some agencies, ISOO is encouraged by the progress from last year.

Agencies reported on the percentage of personnel who meet requirements of E.O. 13526 and 32 CFR Part 2001 relating to training and performance evaluations:

» **Initial Training.** All cleared agency personnel are required to receive initial training on basic security policies, principles, practices, and criminal, civil, and administrative penalties. (32 CFR 2001.70(b))

  - 86.96 percent of the agencies reported that 100 percent of their cleared personnel received this training.

» **Refresher Training.** Persons who apply derivative classification markings are required to receive training in the proper application of the derivative classification principles of E.O.

13526, prior to derivatively classifying information and at least once every two years thereafter. (E.O. 13526, Sec. 2.1(d) and 32 CFR 2001.70(d))

- 47.83 percent of the agencies reported that 100 percent of their cleared personnel received this training.

» **Original Classification Authority (OCA) Training.** OCAs are required to receive training in proper classification and declassification each calendar year. (E.O. 13526, Sec. 1.3(d) and 32 CFR 2001.70(c))

- 54.55 percent of the agencies reported that 100 percent of their OCAs received this training.

» **Derivative Classifier Training.** Persons who apply derivative classification markings are required to receive training in the proper application of the derivative classification principles of E.O. 13526, prior to derivatively classifying information and at least once every two years thereafter. (E.O. 13526, Sec. 2.1(d) and 32 CFR 2001.70(d))

- 61.11 percent of the agencies reported that 100 percent of their derivative classifiers received this training.

» **Performance Element.** The performance contract or other rating system of original classification authorities, security managers, and other personnel whose duties significantly involve the creation or handling of classified information must include a critical element to be evaluated relating to designation and management of classified information. (E.O. 13526, Sec. 5.4(d)(7))

- 30.43 percent of the agencies report that 100 percent of the required personnel have this element.

In addition, agencies reported on whether they meet the requirements of E.O. 13526 that relate to the limiting of OCA delegations and the establishment of classification challenge procedures:

» **OCA Delegations.** Delegations of original classification authority shall be limited to the minimum required to administer E.O. 13526. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority. (E.O. 13526, Sec. 1.3(c)(1))

- 85.0 percent of the agencies with OCA reported that delegations are limited as required.

» **Classification Challenge Procedures.** An agency head or SAO shall establish procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. (E.O. 13526, Sec. 1.8(b))

- 71.74 percent of the agencies reported that they have established classification challenge procedures.

Agencies also reported with regard to the application of marking requirements that were new when E.O. 13526 was issued in 2009:

» **Identification of Derivative Classifiers.** Derivative classifiers must be identified by name and position, or by personal identifier on each classified document. (E.O. 13526, Sec. 2.1(b)(1) and 32 CFR 2001.22(b))

- A total of 35,503 documents were reviewed to evaluate the application of this requirement.
- Agencies reported that 73.36 percent of the documents meet this requirement.

» **Listing of Multiple Sources.** A list of sources must be included on or attached to each derivatively classified document that is classified based on more than one source document or classification guide. (32 CFR 2001.22(c)(1)(ii))

- A total of 30,035 documents were reviewed to evaluate the application of this requirement.
- Agencies reported that 74.84 percent of the documents meet this requirement.

Clearly, many agencies must make improvements in fundamental elements of the program under E.O. 13526 and 32 CFR Part 2001. Many of the above requirements were already in existence when E.O. 13526 was issued in 2009. Those that were established by E.O. 13526 are no longer new. Agencies have had many opportunities to familiarize themselves with these requirements, including briefings held by ISOO after E.O. 13526 was issued, ISOO notices and training materials covering some of these requirements, and interactions between agency personnel and ISOO liaisons. ISOO will advise agencies of these shortfalls and of the importance of meeting these requirements, but agencies that have reported deficiencies should already recognize that they must take corrective actions. Agencies must use their self-inspections to evaluate and improve their classified national security information program. ISOO will continue to use the self-inspection reporting requirements to prompt agencies to do this and to bring their attention to the requirements of E.O. 13526 and 32 CFR Part 2001.

# Interagency Security Classification Appeals Panel

## Mandatory Declassification Review (MDR) Appeals

During FY 2013, 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, 32 CFR Part 2003. The Panel decided upon 46 MDR appeals, containing a total of 151 documents. The documents within these MDR appeals were classified either in part or in their entirety. The Panel affirmed the prior agency classification decisions in 20 documents (13.25 percent), declassified 55 documents (36.42 percent) in their entirety, and declassified 76 documents (50.33 percent) in part.

Since May 1996, the Panel has acted on a total of 1,509 documents. Of these, the Panel declassified additional information in 70 percent of the documents. Specifically, the Panel declassified 409 documents (27 percent) in their entirety, declassified 640 documents (42 percent) in part, and fully affirmed the declassification decisions of agencies in 460 documents (31 percent).

## Classification Challenge Appeals

During FY 2013, the Panel adjudicated two classification challenge appeals filed by authorized holders of classified information, as provided for in section 1.8 of the Order. In each of these appeals, the ISCAP affirmed the classifying agency's original determination.

## Exemptions from Declassification

Section 3.3 (h) of the Order required significant revisions to agency exemptions to automatic declassification by the end of December 2012. 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. Throughout FY 2012 and FY 2013, the Panel approved 23 guides. In FY 2013, ISOO published the results of the declassification guide approval process as ISOO Notice 2013-02, listing those agencies eligible to exempt information at 25, 50, and 75 years.

## ISCAP Decisions Website

In September 2012, the ISCAP Staff created a new website 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 website is the most efficient way for the Panel to provide senior agency officials (and agency declassification staffs) and the public with its decisions and fulfill this requirement. The Panel will supplement and refine the website as the Panel and agencies declassify and release additional information. Refinements in FY 2013 included the development of a search capability for Panel releases and the posting of decisions at the document, rather than appeal, level.

## 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*

John W. Ficklin
*National Security Council Staff*

Michael Higgins
*Department of Defense*

Mark A. Bradley
*Department of Justice*

Margaret P. Grafeld
*Department of State*

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 2013.*

## Support Staff

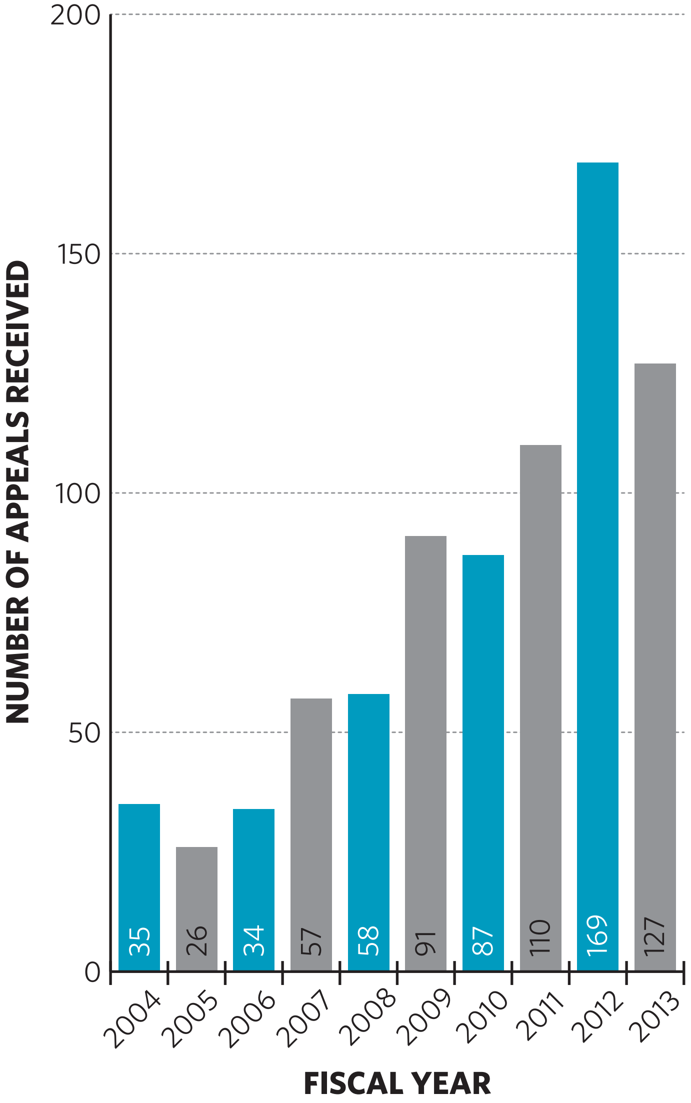
Information Security Oversight Office

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

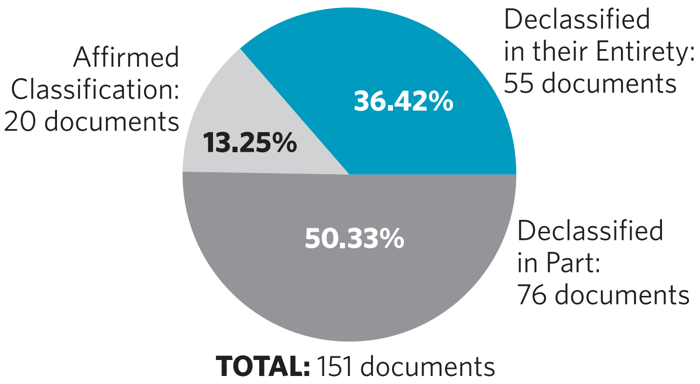
Telephone: 202.357.5250
Fax: 202.357.5908
E-mail: iscap@nara.gov

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

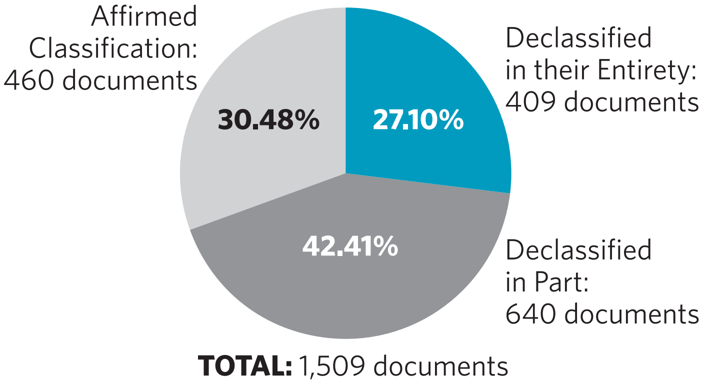
## Number of Appeals Received by ISCAP, FY 2004 – FY 2013



## ISCAP Decisions, FY 2013



## ISCAP Decisions, May 1996 – September 2013



# Cost Estimates for Security Classification Activities

## Background and Methodology

ISOO reports annually to the President on the estimated costs associated with agencies' implementation of 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 2013 is $11.63 billion. For the first time, we have included in this top-line figure the cost estimates of the Intelligence Community (IC)*, which total 1.87 billion. So that a comparison to prior year reports can be made, the total of all of government minus the IC is $9.76 billion, a decrease of $9.9 million, or .1 percent, from FY 2012. The IC costs comprise 16 percent of the total Government costs, an order of magnitude roughly equivalent to that of past years when the IC cost estimates were reported but not disclosed in the top-line figure.

For FY 2013, agencies reported $1.52 billion in estimated costs associated with Personnel Security, an increase of $139.39 million, or 10 percent. The majority of this increase is attributed to an increased number of periodic security clearance reinvestigations.

Estimated costs associated with Physical Security were $2.31 billion, an increase of $617 million, or 36 percent. Increased costs were due primarily to purchase and installation of security equipment and construction of secure facilities.

Estimated costs associated with Classification Management were $353.98 million, an increase of $26.38 million, or 8 percent.

Estimated costs associated with Declassification were $99.77 million, an increase of $51.11 million, or 105 percent. This is due to an increase in declassification activity in numerous agencies.

Estimated costs associated with Protection and Maintenance for Classified Information Systems were $4.40 billion, an increase of $368.49 million, or 9 percent.

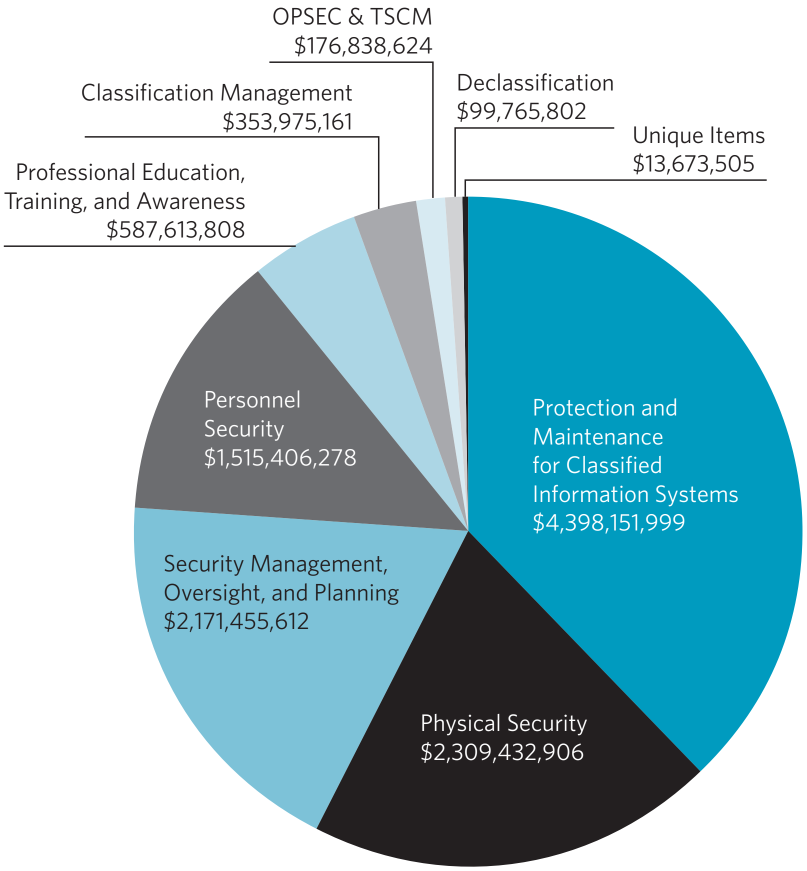
Estimated costs associated with OPSEC and TSCM were $176.84 million, an increase of $52.38 million, or 42 percent. The increase is due to the establishment of a new TSCM program.

The estimated costs for Professional Education, Training, and Awareness were $587.61 million, an increase of $157.33 million, or 37 percent.

Estimated costs associated with Security Management, Oversight, and Planning were $2.17 billion, an increase of $442.70 million, or 26 percent.

Estimated costs associated with Unique Items were $13.67 million, an increase of $165,401, or 1 percent.

### Government Security Classification Costs, FY 2013



**TOTAL:** $11,626,313,695

*Note: Includes cost estimates from the Intelligence Community.*

**The IC elements include 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*

## Government Security Classification Costs, FY 1995 – FY 2013

| Year | 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 |
| 2013 | $1.52 billion | $2.31 billion | $353.98 million | $99.77 million | $4.40 billion | $176.84 million | $587.61 million | $2.17 billion | $13.67 million | $11.63 billion |

**Prior to 1998, Declassification costs were included in Classification Management costs.*

*+Prior to 2003, OPSEC and TSCM costs were not reported.*

*Note: As of FY 2013, Intelligence Community costs are included.*

## 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 2013, the Defense Security Service collected industry cost data and provided the estimate to ISOO.

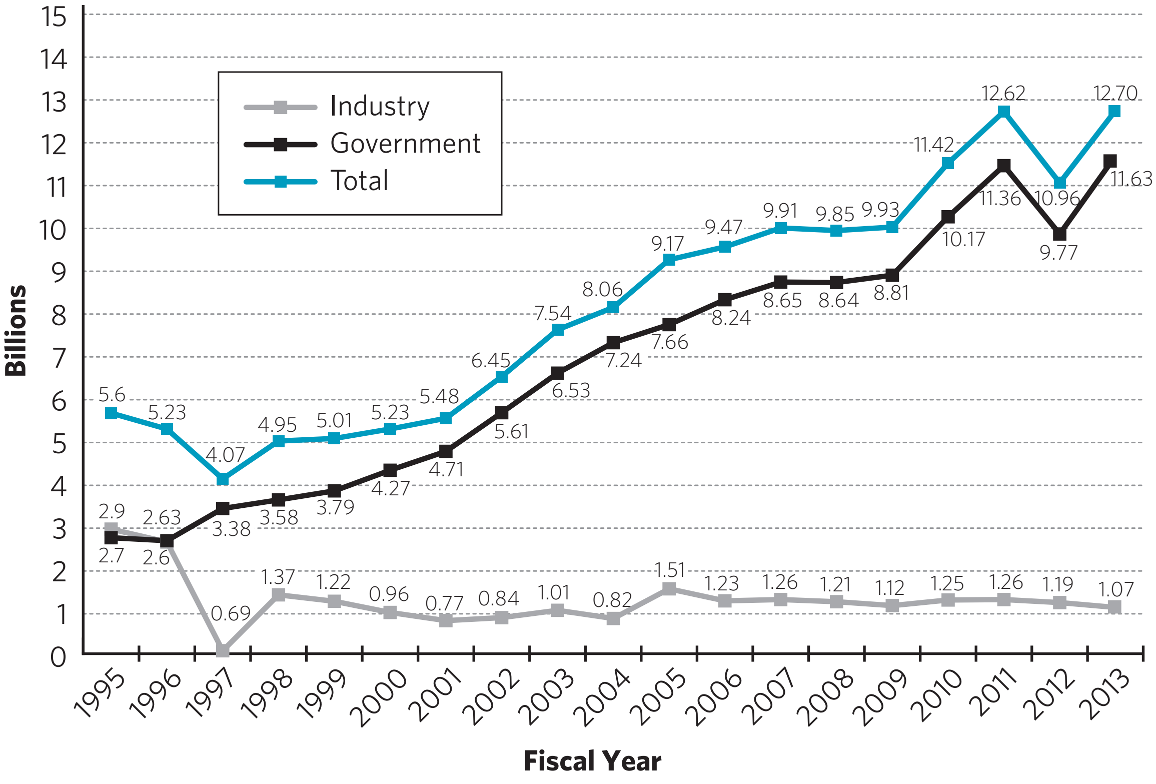
Cost estimate data are not provided by category because industry accounts for its costs differently than Government. Rather, a sampling method was applied that included volunteer companies from four different categories of facilities. The category of facility is based on the complexity of security requirements that a particular company must meet in order to hold and perform under a classified contract with a Government agency.

The FY 2013 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 2013 within industry was $1.07 billion; a decrease of $126.02 million, or 11 percent.

## Results—Combined Government and Industry

This year's combined estimate for Government and industry was $12.70 billion, an increase of $1.73 billion, or 16 percent.

### Total Costs for Government and Industry, FY 1995 – FY 2013



*Note: Includes cost estimates from the Intelligence Community.*

# The National Industrial Security Program

ISOO is responsible for implementing and overseeing the National Industrial Security Program (NISP) mandated under E.O. 12829, as amended. 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 the NISP executive order. Membership of the NISPPAC is comprised of both Government and industry representatives, and 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 is required to convene at least twice a calendar year at the discretion of the Director of ISOO or the Designated Federal Official for the NISPPAC. NISPPAC meetings are open to the public and administered in accordance with the Federal Advisory Committee Act.

The NISPPAC met three times during FY 2013. The major issues discussed during these NISPPAC meetings included the timeliness of processing contactor personnel security clearances, the certification and accreditation of information systems processing classified information, industry implementation of national insider threat policies, national cyber security initiatives and the revision of the NISPOM and 32 CFR Part 2004, NISP Directive No.1, to incorporate required changes.

The NISPPAC convenes several government/industry working groups to address NISPPAC 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. The continuing work of these groups is reported at each NISPPAC meeting.

The Personnel Security Clearance working group continues to review and analyze a comprehensive set of metrics that measure the efficiency and effectiveness of security clearance processing for industry. The working group review includes metric data from the Office of Personnel Management (OPM), the Office of the Director of National Intelligence, the Departments of Energy and Defense, and the Nuclear Regulatory Commission. The working group is an important venue to examine performance, discuss opportunities to improve, and keep stakeholders informed about emerging issues. These include upgrades to the OPM's e-QIP system for on-line clearance submittals, requirements for electronic fingerprinting submittals, and potential changes to the security clearance process resulting from both the Washington Navy Yard shooting and the wave of recent unauthorized disclosures.

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 continues to recommend changes to policies and standards and tracks performance metrics to monitor the consistency, timeliness, and effectiveness of the C&A processes.

The E.O. 13587 working group was established to develop and propose changes to policy and guidance pursuant to the issuance of E.O. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. This group works to ensure that structural reforms mandated in E.O. 13587, as well as the National Insider Threat Policy, are fully integrated into NISP processes and implementation standards for contractors, grantees and licensees.

The issuance of E.O. 13526 created a need to revise portions of the NISPOM. To maximize the effectiveness of this rewrite effort, the NISPPAC working with DoD, as the NISP executive agent, the Cognizant Security Agencies, and other affected agencies, were provided an opportunity to review and recommend revisions to existing guidelines and proposed changes. A conforming change to the current NISPOM was issued in FY 2013 and a comprehensive updated NISPOM will be issued in FY 2015.

The potential impact of the implementation of Controlled Unclassified Information (CUI) program 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.

Finally, during FY 2013, we continued our outreach and support to a myriad of industrial security entities, to include the National Classification Management Society, Aerospace Industries Association-National Defense Intelligence Council, ASIS International, and Industrial Security Awareness Councils.

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

# Controlled Unclassified Information

*A standardized methodology that permits maximum flexibility in application is being developed to service the widest range of both information and users.*

## Background

Executive Order 13556, "Controlled Unclassified Information," (the Order[1]) established the Controlled Unclassified Information (CUI) program to standardize the way the Executive branch handles Sensitive But Unclassified (SBU) information while emphasizing and enhancing the openness, transparency, and uniformity of government-wide practices. ISOO manages the CUI program and fulfills the Executive Agent (EA) responsibilities designated by the Order to NARA.

Following issuance of the Order, the EA published baseline requirements for agency-specific CUI policies and procedures, and Federal agencies reviewed their respective SBU information practices and submitted to the EA those categories and subcategories that the agency would like to continue to employ. The EA reviewed more than 2,200 proposed category and subcategory submissions from 47 agencies and led interagency discussions to consolidate redundancies and provide consistency among like categories. Categories and subcategories are defined in the CUI Registry. The Registry also includes citations for law, Federal regulation and government-wide policy that authorize control of each defined category and subcategory and, when fully developed, will serve as the primary source of direction for marking and handling CUI.

## Policy Development

In FY 2013, the EA advanced the iterative policy development strategy launched in FY 2012, interspersing working group discussions, surveys and consolidation of current practices, initial drafting, informal agency comment, and EA comment adjudication for individual policy elements. This process has created a substantial body of internal research and analysis for incorporation into the program.

Promoting full participation of all CUI stakeholders reiterated the challenge of developing and coordinating a policy that addresses the broad spectrum of information types identified as CUI, and the wide range of responsibility levels of potential designators and recipients of CUI (Federal, state, local, tribal, non-governmental). Some CUI users have comprehensive experience with the concepts of protected information in a classified environment; for others, the need to be aware of safeguarding and dissemination requirements for sensitive information is seldom a factor in day-to-day operations. A standardized methodology that permits maximum flexibility in application is being developed to service the widest range of both information and users.

In May 2013, ISOO issued *CUI Notice 2013-01: Provisional Approval of CUI Categories and Subcategories*, based on discussion with the Office of Management and Budget (OMB). This Notice establishes a process for the CUI EA to provisionally approve categories and/or subcategories for information types that reasonably require the protections of the CUI program but currently lack a statutory, regulatory, or Government-wide basis for control. Provisional approval will permit agencies to more efficiently and effectively plan for program implementation by allowing CUI planning activities to be performed in tandem with agency development of an enactment that meets the requirements of the Order.

The CUI Advisory Council (the Council) was established in June 2013

[1] Executive Order 13556 "Controlled Unclassified Information," dated November 4, 2010.

to carry out the consultative functions directed by Executive Order 13556 and to advise the CUI EA on the development and issuance of policy and implementation guidance for the CUI program. The Council is chaired by the Director of ISOO, and current membership is based on that of the Chief Financial Officers' Council with representatives from 28 agencies; others attend by invitation.

With formal input from the Council and Council-nominated subject matter experts, policy is being developed concurrently on multiple levels:

1. Implementing directive to be incorporated into the Code of Federal Regulations (CFR) will include principles and guidelines applicable to all information and users;
2. Supplemental Guidance, including, but not limited to, procedures, definitions and protocols for appropriate safeguarding, dissemination, marking, and decontrol of unclassified information; and
3. Expansion of the CUI Registry to reflect additional authorized categories and subcategories, markings, designation authorities, specified CUI requirements and a glossary of terms.

Implementation of the CUI program is being planned along a phased timeline, and will include responsibilities for both the EA and agencies. A target date for Initial Operating Capability (IOC), defined as the ability to recognize CUI and to receive CUI for physical safeguarding, will be established based upon publication of the CFR, and will be uniform across all agencies in the Executive branch. Full Operating Capability (FOC) will be achieved on an agency-by-agency basis, based on each agency completing all implementation tasks, including necessary information technology updates.

## CUI PHASED IMPLEMENTATION

Day 0: FY15 Day 180: FY16 Year 1: FY16 Year 3-4: FY18-19

| | Planning | Readiness | Initiation | Final |
|---|---|---|---|---|
| Phases | Identify and initiate planning activities for CUI implementation | Prepare environment and workforce for the CUI transition | Begin implementation of CUI practices<br>Begin Phase Out of obsolete practices | Full Implementation of the CUI program |
| Key EA Activities | • Publish 32 CFR Part 2002 Rule & Supplemental Guidance (Day 0)<br>• Augment Registry<br>• Provide Awareness Materials & Products<br>• Consult with OMB & Provide Budget Guidance<br>• Review Agency Policies | • Publish Training (Day 180)<br>• Provide Additional Guidance as needed<br>• Establish Schedule for On-site Reviews<br>• Provide Training Support & Consultation | • Oversee Executive Branch Implementation<br>• Resolve Disputes & Complaints<br>• Initiate On-site Reviews | • Oversee Executive Branch Implementation<br>• Collect Reporting Data |
| | Monitor & Report on Phased Implementation | | | |
| Key D/A Activities | • **Develop & Publish Policy***<br>• Develop Training<br>• Plan for FY16-18 Budget Cycles<br>• Develop IT Transition Plan<br>• Develop Self-Inspection Plan<br>• Develop Process to Assess Agency Compliance<br>• Develop Process to Manage CUI Status Challenges | • **Assert Physical Safeguarding***<br>• **Conduct Training***<br>• Initiate Awareness<br>• Continue Budget Cycle Planning<br>• Prepare IT Transition<br>IOC | • Initiate CUI Implementation<br>• Handle<br>• Recognize<br>• Receive<br>• Initiate IT Transition<br>• Permit Creation of CUI<br>• Initiate Self-Inspection Program | • Eliminate Old Markings<br>• Assure use of only New Markings<br>• Complete IT Transition<br>• Monitor & Report Implementation<br>FOC |

* Required for Initial Operating Capability (IOC)

The CUI EA is currently editing the draft implementing directive based on final informal agency comment and anticipates that it will enter the formal OMB-managed comment process in coming months. Based on CUI Advisory Council meetings, implementation planning workshops, and consultation with OMB, the CUI EA will develop a National Implementation Plan that will include target dates for phased implementation.

## Training and Outreach

To maintain timely communication with stakeholders, in April 2013, ISOO requested that agencies affirm or update their designation of a Senior Agency Official (SAO) responsible for the implementation of their respective CUI program, and to designate a Program Manager (PM) to serve as their agency's primary interface with ISOO in its role as the CUI EA. An overview and summary of the current state of the CUI program, tailored to these new SAOs and PMs, was presented in July 2013.

Also in July, ISOO conducted a specialized workshop on CUI training to collaborate with impacted agencies, determine implementation work plan activities, and identify (phased implementation) target dates for training. During the summer of 2013, the CUI EA requested information from stakeholders to serve as a planning aid for Executive branch-wide implementation. The data collected for training included identification of existing training programs and requirements, impacted personnel, target audiences, and requirements for future CUI implementation across the Executive branch.

As a follow-up to the FY 2012 issuance of *Guidance Regarding CUI and the Freedom of Information Act*, published jointly by the EA and the Office of Information Policy at the Department of Justice, in February 2013, ISOO issued *Controlled Unclassified Information (CUI) and the Freedom of Information Act (FOIA)*, a computer-based training module clarifying the distinction between the CUI program and the FOIA. The training is designed for all Government employees, and is particularly pertinent to those who will deal directly with CUI markings and designations as well as FOIA provisions and exemptions.

The EA plans to develop and issue CUI baseline training based on final policy and guidance. In preparation, the EA will continue to assess agency training requirements, including technical standards for implementation across the Executive branch. The EA will also continue to develop CUI awareness products and to provide training support and consultation to agencies.

The EA is encouraging agencies to continue planning their training efforts. All CUI training modules are publicly available on the CUI website for either direct access or download. Training source code is available to agencies to allow for mission-specific modification and implementation.

In FY 2013, the CUI EA completed briefing SAOs and their staffs, from all the member departments of the President's Cabinet. Based on their position in the Executive branch and influence over national policy, these stakeholders have the greatest potential to impact the overall implementation of the CUI program. Their implementation of national programs and interaction with the rest of the Federal Government strongly influence independent agencies and other organizations throughout the Executive branch. As an additional outreach effort, ISOO provides overviews and participates in panel discussions within the Federal government, with State, local, and private sector entities, and with public interest groups.

## CUI Registry and Website

The online CUI Registry currently includes descriptions for 22 categories and 85 subcategories of unclassified information, supported by 314 unique control citations and 105 unique sanction citations in the United States Code, Code of Federal Regulations, and government-wide policies. All references were reconfirmed and updated based on annual updates to the United States Code, Code of Federal Regulations and review of government-wide policy documents.

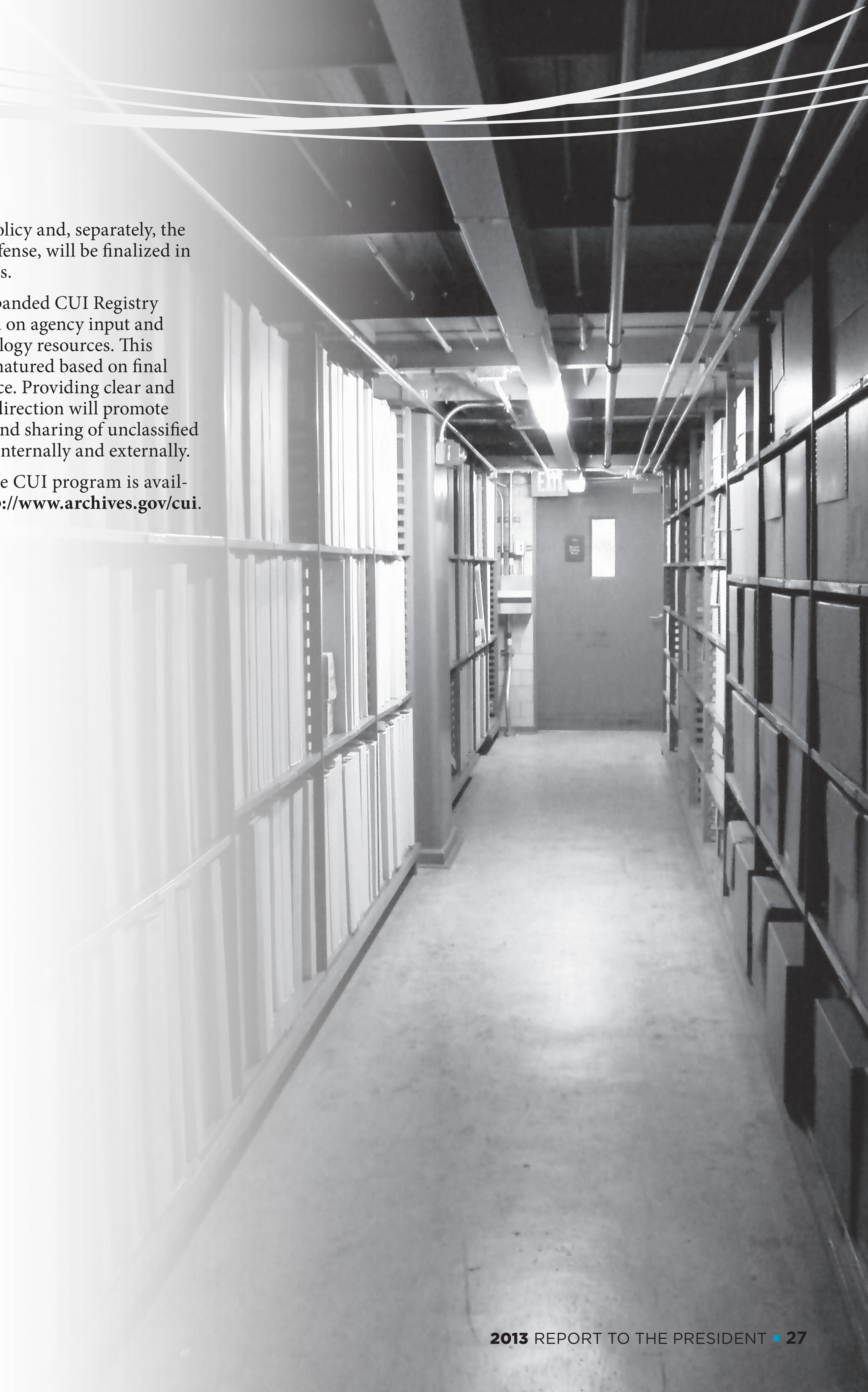
As the repository for common definitions, protocols and procedures for properly marking, safeguarding, disseminating and decontrolling unclassified information, based on law, regulation, and government-wide policy, the CUI Registry is a cornerstone of the CUI program. ISOO led specialized Registry workshops in which agencies were provided opportunities to submit input for potential consideration as additional Registry capability.

In addition to the online CUI Registry, an active web presence provides updates, handouts, answers to frequently asked questions about the CUI program, an overview of governance structure, a listing of CUI Advisory Council members, CUI documents, memoranda, and reports.

The EA will continue to update the CUI Registry based on identification of unclassified information that requires protection based on law, regulations, and/or government-wide policies. It is anticipated that new categories currently under discussion with the White House Office of Science and Technology Policy and, separately, the Department of Defense, will be finalized in the coming months.

Redesign of an expanded CUI Registry is underway, based on agency input and anticipated technology resources. This approach will be matured based on final policy and guidance. Providing clear and readily accessible direction will promote better protection and sharing of unclassified information both internally and externally.

Information on the CUI program is available online at **http://www.archives.gov/cui**.



ISOO

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