2014 | REPORT *to the* PRESIDENT

ISOO

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. 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

May 29, 2015

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 2014, 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 National Industrial Security Program, the Controlled Unclassified Information Program, and the cost of security classification activity.

ISOO fulfills Executive Agent (EA) responsibilities for the CUI Program, which were designated by Executive Order 13556 to the National Archives and Records Administration. During the past year, ISOO continued to advance its policy development strategy, and submitted a proposed Federal CUI rule (the future 32 Code of Federal Regulations 2002) into the Office of Management and Budget (OMB)-managed Federal rule-making process. The EA also initiated a CUI Program appraisal process to assist Executive branch agencies in preparing for implementation by providing agency planners with a baseline. In addition, the EA developed an updated training module clarifying the distinction between the CUI Program and the provisions of the Freedom of Information Act.

We successfully partnered with the National Institute of Standards and Technology (NIST) to produce a joint publication, NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organization." This publication, expected to be finalized in 2015, provides information system protection standards for CUI in the non-Federal environment. After completion of the CUI Federal rule and NIST publication, we will propose a Federal Acquisition Regulation rule to provide agencies with a standard approach for applying these CUI requirements to their contractors. The EA plans to issue a National Implementation Plan for the executive branch, which will provide a timeline of phased 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 had another successful year adjudicating declassification appeals and posting the decisions on a publicly available website. The Panel decided upon 451 documents that had been received as mandatory declassification review appeals. Furthermore, the Panel has now posted 538 documents to its online database that serves to inform the public and agency declassification reviewers of the Panel's decisions.

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 (NISP) policy and guidance.

In other NISP focus areas, ISOO continues its contribution to government-wide security and suitability process reform efforts through membership in the Suitability and Security Clearance Performance Accountability Council (PAC) and the PAC Advisory Council. Lastly, ISOO also contributed significant support to administration cybersecurity information sharing initiatives, guiding NISP partner agencies through the creation of novel risk-management processes made effective as part of Executive Order 13691 "Promoting Private Sector Cybersecurity Information Sharing." ISOO is poised to continue its support to these and future reforms.

Respectfully,

John P. Fitzpatrick

JOHN P. FITZPATRICK
Director

★ TABLE *of* CONTENTS ★

On the cover: Fort McHenry, Baltimore, Maryland, in honor of the 200th anniversary of America's national anthem. In September 1814, while aboard a British ship to negotiate the release of prisoners, Francis Scott Key watched as the British bombed Fort McHenry. Despite 25 hours of continuous bombing, Key observed that the American flag was still flying. Back in Baltimore, he quickly composed a poem, which was soon handed out as a handbill under the title "Defence of Fort McHenry." Later, the words were set to music, and the tune was titled "The Star Spangled Banner."

SUMMARY *of* FY 2014 PROGRAM ACTIVITY

Classification

Executive branch agencies reported 2,276 original classification authorities (OCA), up from 2,269 reported in FY 2013.

Agencies reported 46,800 original classification decisions, a decrease of 20 percent.

Agencies reported using the ten-years-or-less declassification instruction for 40 percent of original classification decisions.

Executive branch agencies reported 77,515,636 derivative classification decisions; a 3 percent decrease from FY 2013.

Declassification

Agencies received 9,026 initial mandatory declassification review (MDR) requests and closed 7,798 requests. The average number of days to resolve each request is 224. A total of 11,123 requests have remained unresolved for over one year. This number includes requests that have been carried over from prior years. Agencies reviewed 597,498 pages, and declassified 372,134 pages in their entirety, declassified 190,654 pages in part, and retained classification of 34,710 pages in their entirety.

Agencies received 409 MDR appeals and closed 286 appeals. The average number of days to resolve each appeal is 296. A total of 475 appeals have remained unresolved for over one year.

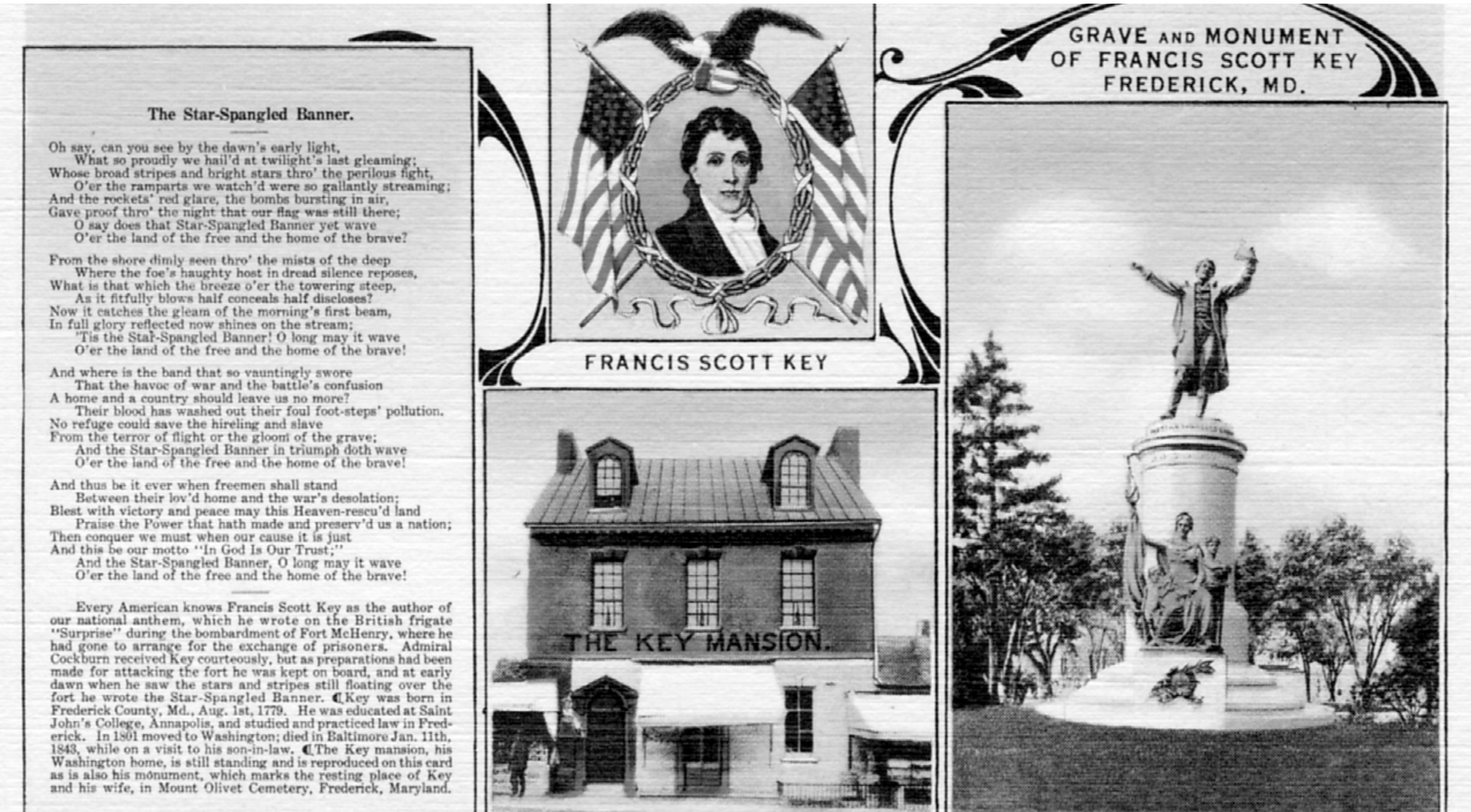
Agencies reviewed 41,337 pages on appeal, and declassified 20,756 pages in their entirety, declassified 15,236 pages in part, and retained classification of 5,345 pages in their entirety.

Under automatic declassification, agencies reviewed 60,491,810 pages and declassified 25,660,183 pages of historically valuable records.

Under systematic declassification reviews, agencies reviewed 3,933,823 pages, and declassified 2,093,258 pages.

Under discretionary declassification reviews, agencies reviewed 201,375 pages, and declassified 65,825 pages.

Under automatic, systematic, and discretionary declassification reviews, a total of 64,627,008 pages were reviewed for declassification and 27,819,266 pages were declassified.


GRAVE AND MONUMENT
OF FRANCIS SCOTT KEY
FREDERICK, MD.
FRANCIS SCOTT KEY
THE KEY MANSION.

The Star-Spangled Banner.

Oh say, can you see by the dawn's early light,
What so proudly we hail'd at twilight's last gleaming;
Whose broad stripes and bright stars thro' the perilous fight,
O'er the ramparts we watch'd were so gallantly streaming;
And the rockets' red glare, the bombs bursting in air,
Gave proof thro' the night that our flag was still there;
O say does that Star-Spangled Banner yet wave
O'er the land of the free and the home of the brave?

From the shore dimly seen thro' the mists of the deep
Where the foe's haughty host in dread silence reposes,
What is that which the breeze o'er the towering steep,
As it fitfully blows half conceals half discloses?
Now it catches the gleam of the morning's first beam,
In full glory reflected now shines on the stream;
'Tis the Star-Spangled Banner! O long may it wave
O'er the land of the free and the home of the brave!

And where is the band that so vauntingly swore
That the havoc of war and the battle's confusion
A home and a country should leave us no more?
Their blood has washed out their foul foot-steps' pollution.
No refuge could save the hireling and slave
From the terror of flight or the gloom of the grave;
And the Star-Spangled Banner in triumph doth wave
O'er the land of the free and the home of the brave!

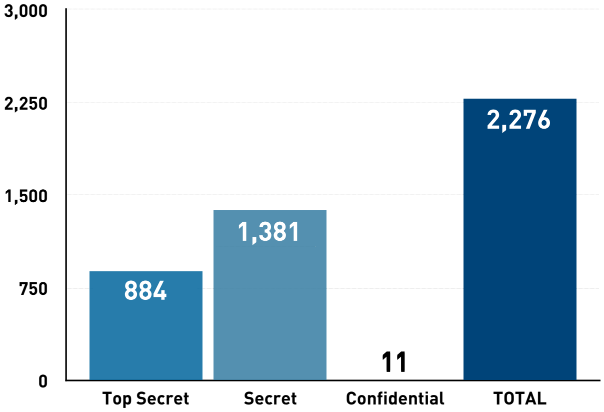
And thus be it ever when freemen shall stand
Between their lov'd home and the war's desolation;
Blest with victory and peace may this Heaven-rescu'd land
Praise the Power that hath made and preserv'd us a nation;
Then conquer we must when our cause it is just
And this be our motto "In God Is Our Trust;"
And the Star-Spangled Banner, O long may it wave
O'er the land of the free and the home of the brave!

Every American knows Francis Scott Key as the author of our national anthem, which he wrote on the British frigate "Surprise" during the bombardment of Fort McHenry, where he had gone to arrange for the exchange of prisoners. Admiral Cockburn received Key courteously, but as preparations had been made for attacking the fort he was kept on board, and at early dawn when he saw the stars and stripes still floating over the fort he wrote the Star-Spangled Banner. ℂKey was born in Frederick County, Md., Aug. 1st, 1779. He was educated at Saint John's College, Annapolis, and studied and practiced law in Frederick. In 1801 moved to Washington; died in Baltimore Jan. 11th, 1843, while on a visit to his son-in-law. ℂThe Key mansion, his Washington home, is still standing and is reproduced on this card as is also his monument, which marks the resting place of Key and his wife, in Mount Olivet Cemetery, Frederick, Maryland.

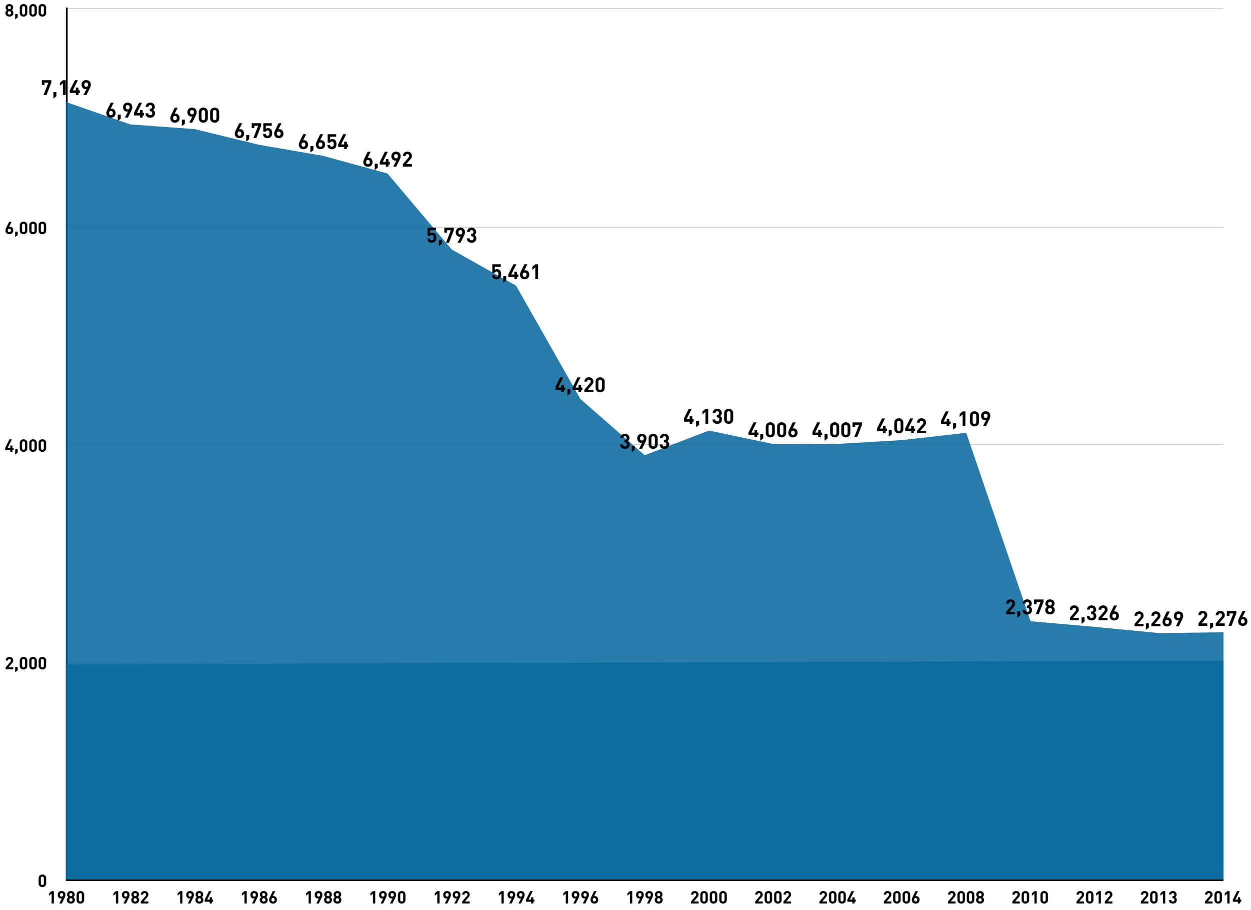
Original Classification Authorities

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 2,276 OCAs in FY 2014; a .31 percent increase from the 2,269 reported in FY 2013.

Original Classification Authorities, FY 2014



Number of Original Classification Authorities FY 1980–FY 2014



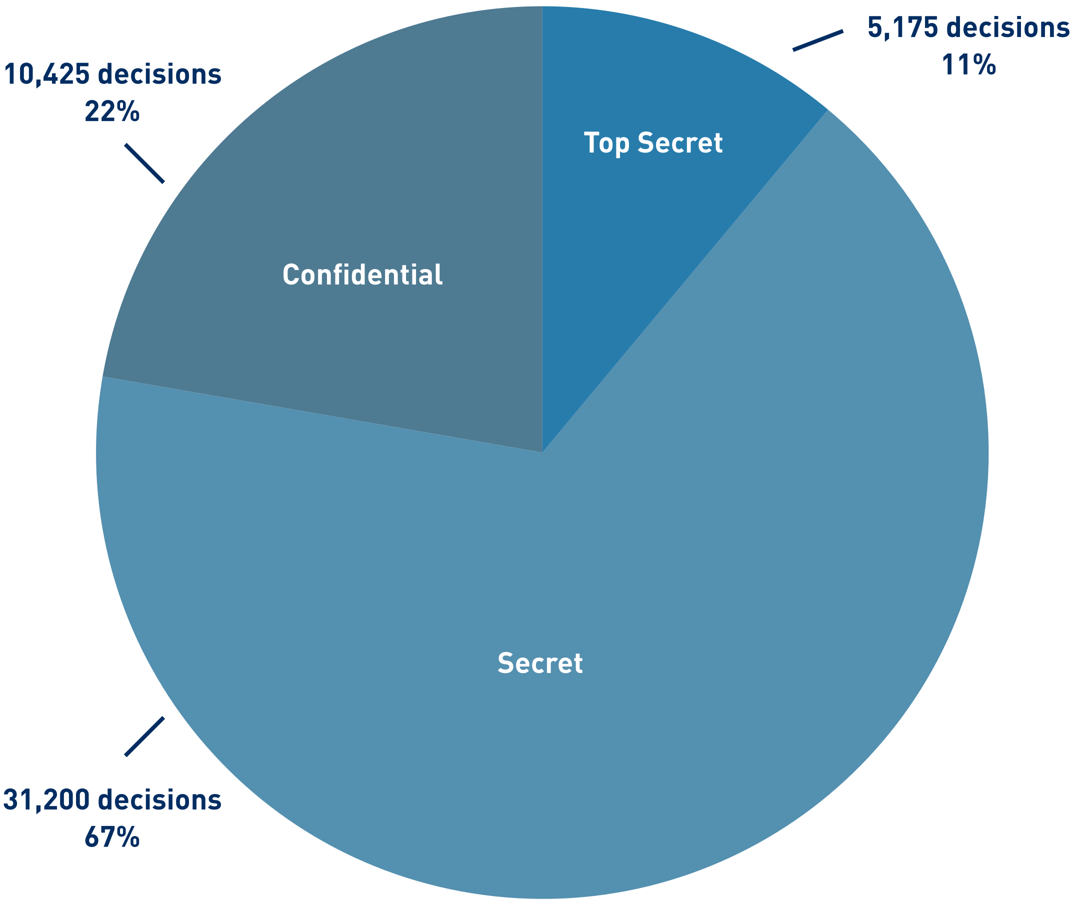
Original Classification

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.

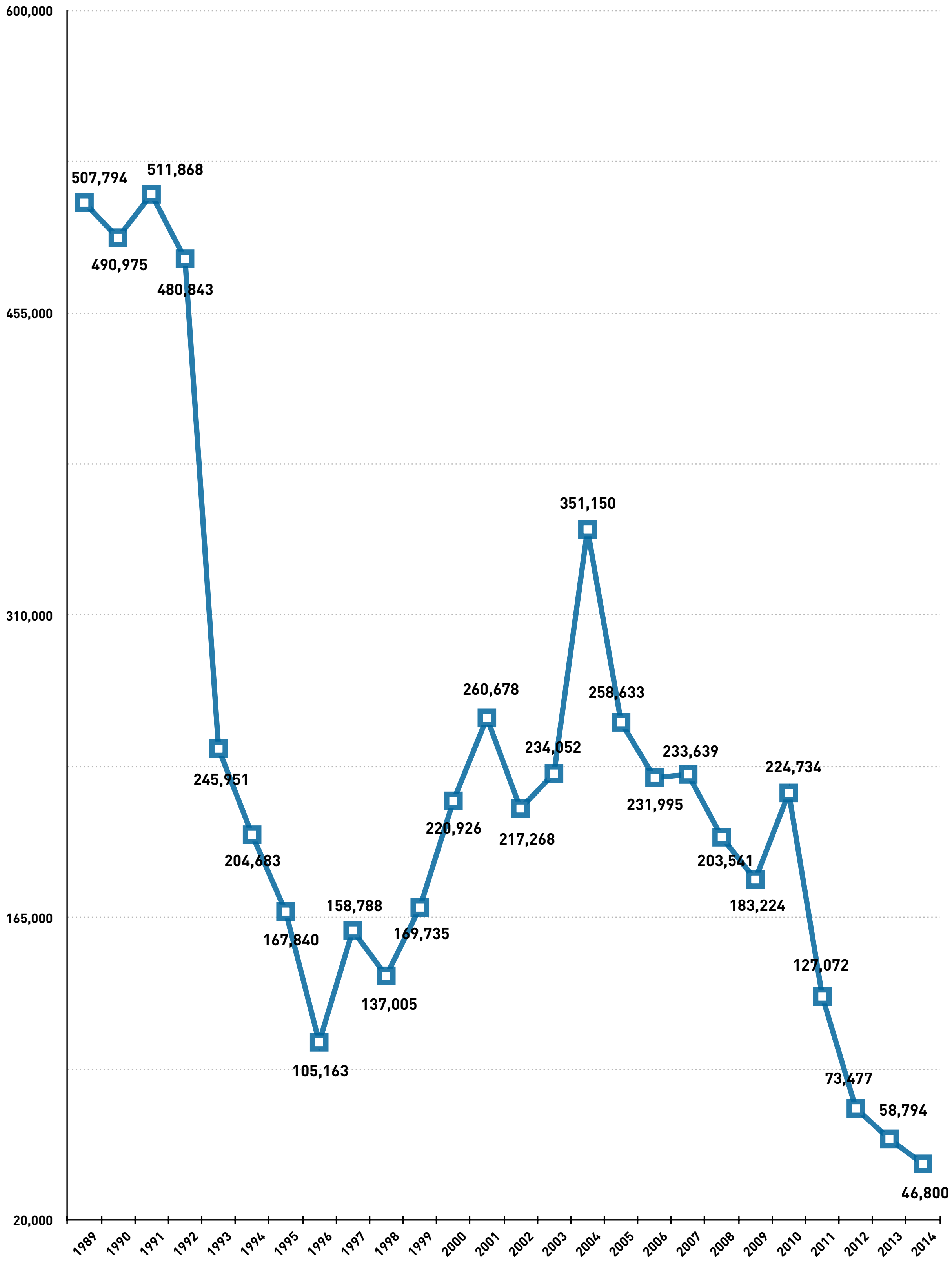
The agencies reported 46,800 original classification decisions for FY 2014, using the ten-years-or-less declassification instruction 40 percent of the time, a decrease of 21 percent from the previous year.

Original Classification Activity
FY 2014

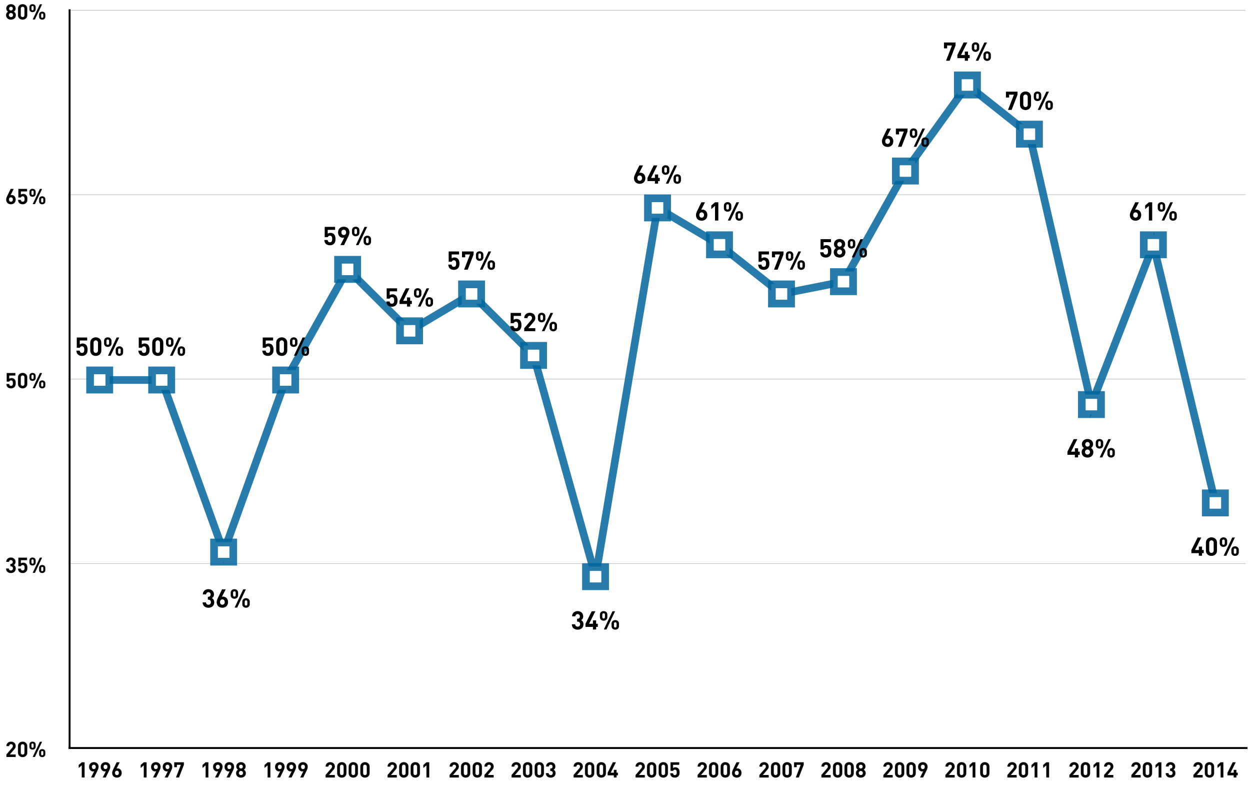


Total: 46,800

Original Classification Activity
FY 1989–FY 2014



Use of the "Ten Years or Less" Declassification Category
FY 1996–FY 2014



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 that identifies 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.

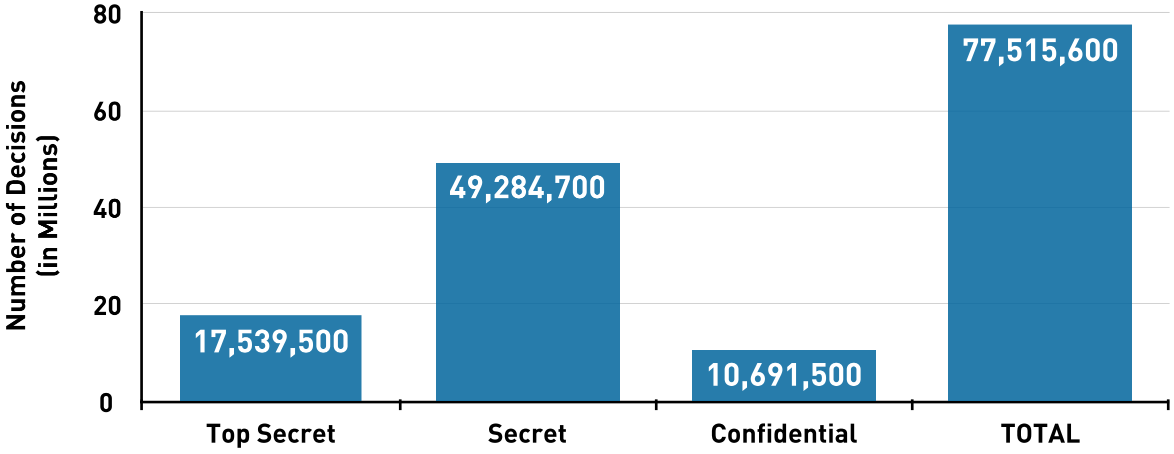
Every derivative classification action is based on information where classification has already been determined by an OCA. Derivative classification decisions must be traceable to the original classification decision made by an OCA. Agencies reported an estimated total of 77.52 million derivative classification decisions in FY 2014, a decrease of 3 percent from FY 2013.

Classification Challenges

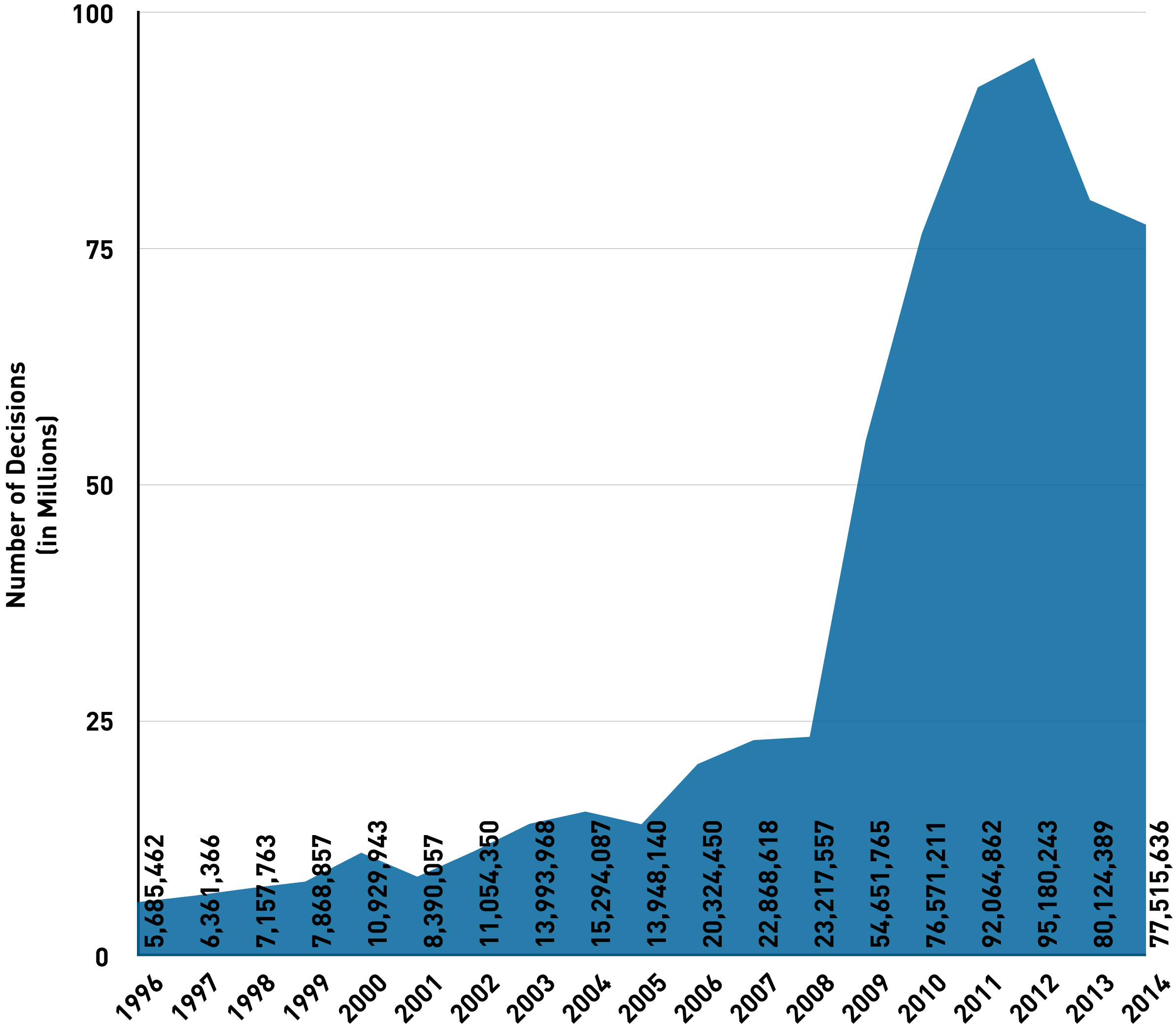
Authorized holders of information who, in good faith, believe its classification status is improper are encouraged and expected to challenge the classification status of that information. Classification challenges are handled both informally and formally, and provide individual holders the responsibility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

Agencies reported 813 formal challenges in FY 2014; 355 (43.67 percent) were fully affirmed at their current classification status with 453 (55.72 percent) being overturned either in whole or in part. Five challenges remain open.

Derivative Classification Activity
FY 2014



Derivative Classification Activity
FY 1996–FY 2014



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 an agency determines 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

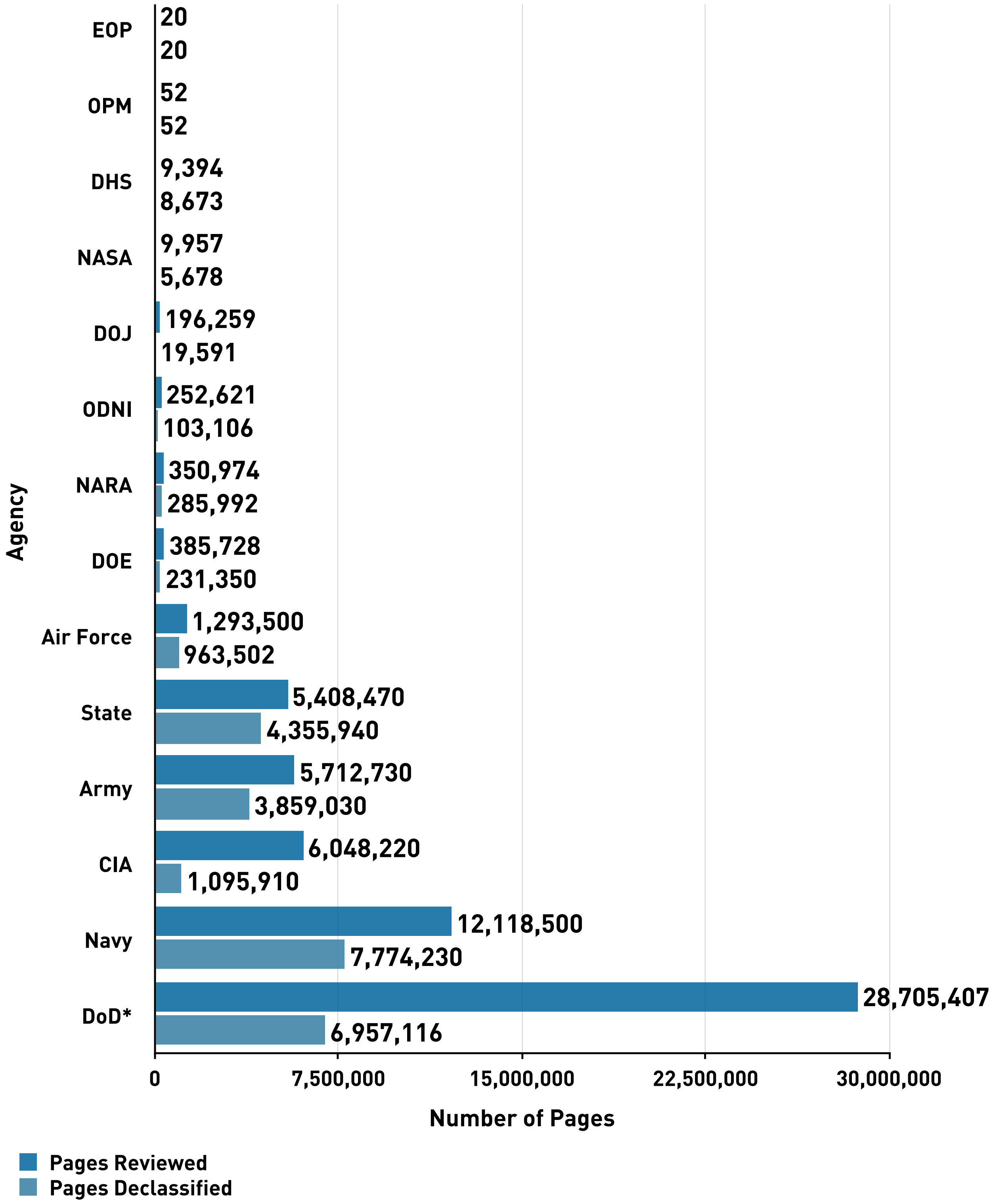
During FY 2014, a total of 64.63 million pages were reviewed under the automatic, systematic, and discretionary declassification programs, and 27.82 million pages (43 percent) were declassified.* This is a 3 percent decrease in the scale of declassification from FY 2013, when 59.33 million pages were reviewed and 27.52 million pages (46 percent) were declassified. While there was a slight decrease in the percentage of pages being declassified, the number of pages reviewed increased by 5.30 million, and the number of pages declassified increased by 294,924.

Under automatic declassification review, agencies reviewed 60.49 million pages and declassified 25.66 million pages (42 percent). Under systematic declassification review, agencies reviewed 3.93 million pages and declassified 2.09 million pages (53 percent). Under discretionary declassification review, agencies reviewed 201,375 pages and declassified 65,825 pages (33 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.

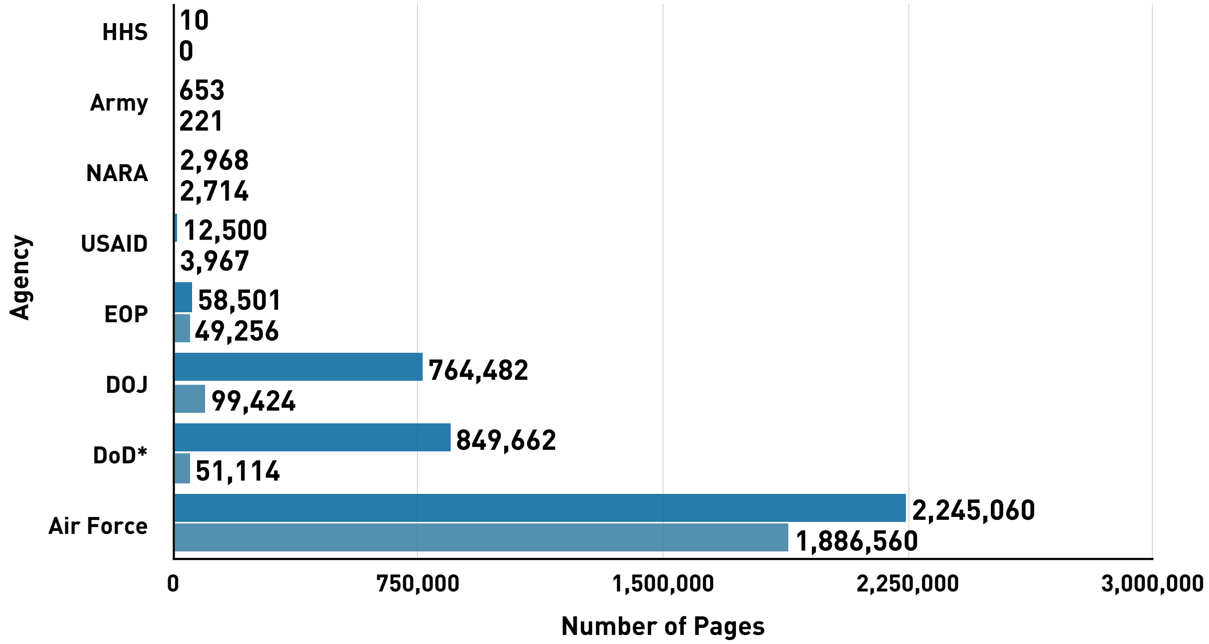
**This data does not include the status of documents processed by the National Declassification Center. Information about that program can be found at* http://www.archives.gov/declassification/ndc/releases.html

Number of Pages Reviewed and Declassified for Automatic Declassification FY 2014

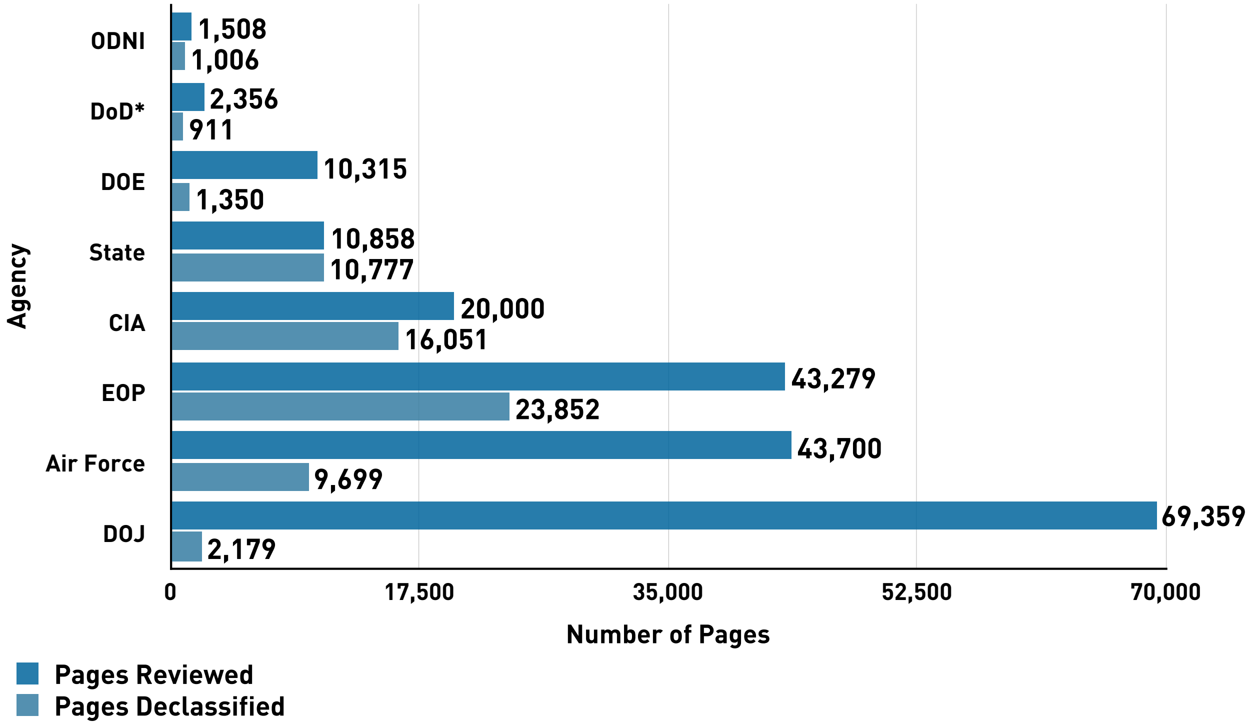


* DOD numbers do not include Air Force, Army, and Navy.

Number of Pages Reviewed and Declassified for Systematic Declassification FY 2014

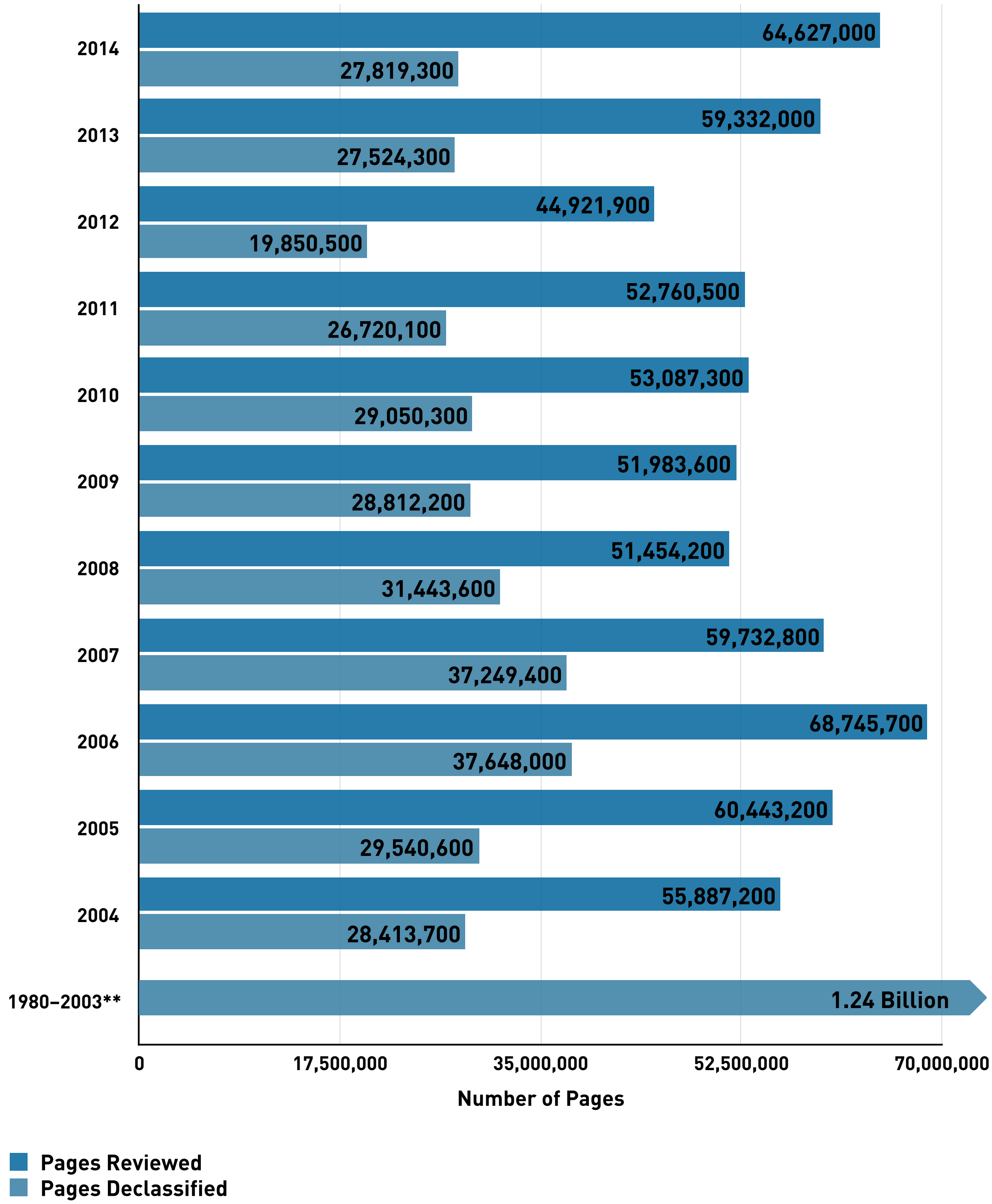


Number of Pages Reviewed and Declassified for Discretionary Declassification FY 2014



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

Total Number of Pages Reviewed and Declassified*
Automatic, Systematic, and Discretionary Declassification Review
FY 1980–FY 2014



* 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.

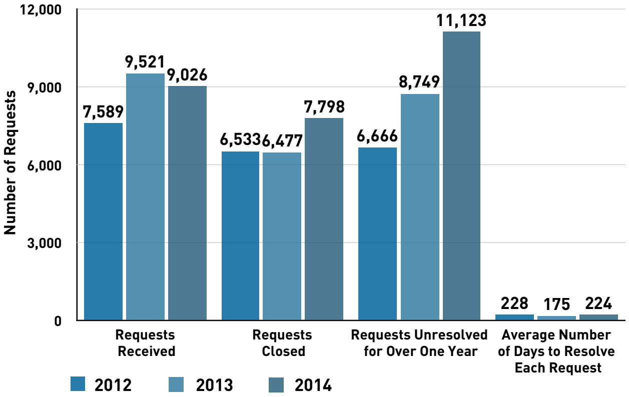
In FY 2012, ISOO implemented a new reporting requirement to measure the response time for MDR requests. Agencies are now asked to report the average number of days it takes for them to close MDR requests. Agencies and ISOO can more clearly understand how agencies are executing their MDR programs successfully 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 2014

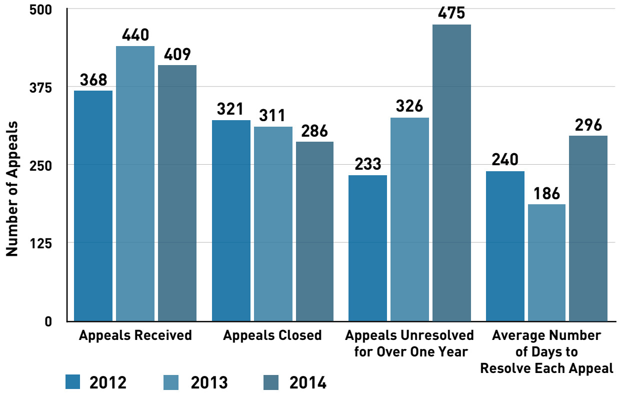
The FY 2014 data specify the number of requests and appeals received, the number that remain unresolved for over one year, and the average number of days it takes to resolve each request and appeal. The report also displays the number of referred MDR requests and appeals to more accurately reflect the MDR workload of agencies. The number of referred MDR requests and appeals are not included in the statistical calculations to prevent duplicate counts.

Mandatory Declassification Review Program Activity FY 2012–FY 2014

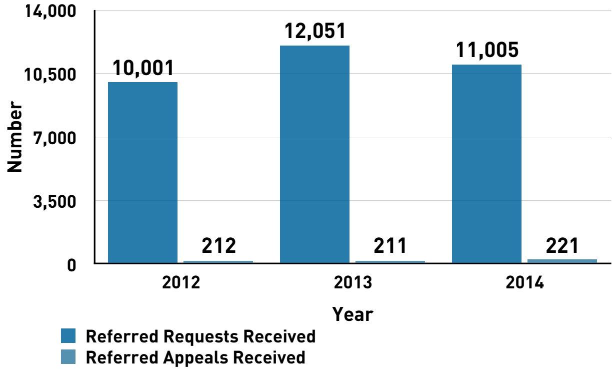
Mandatory Declassification Review Requests



Mandatory Declassification Review Appeals

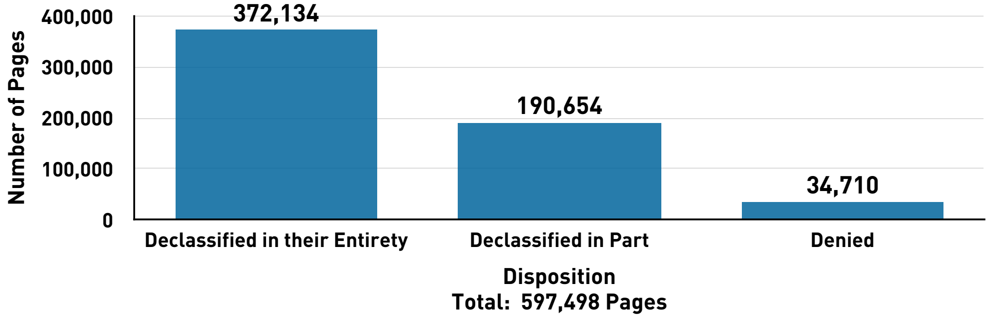


Mandatory Declassification Review Referrals* FY 2012–FY 2014

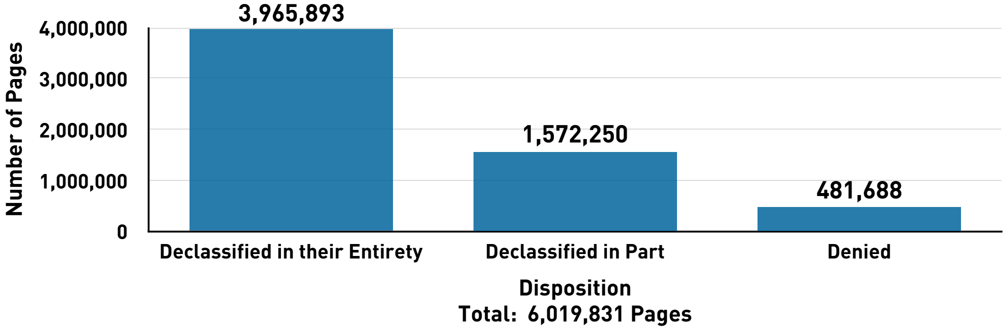


*** MDR requests and appeals referred to an agency from another agency that is responsible for the final release of the request/appeal.**

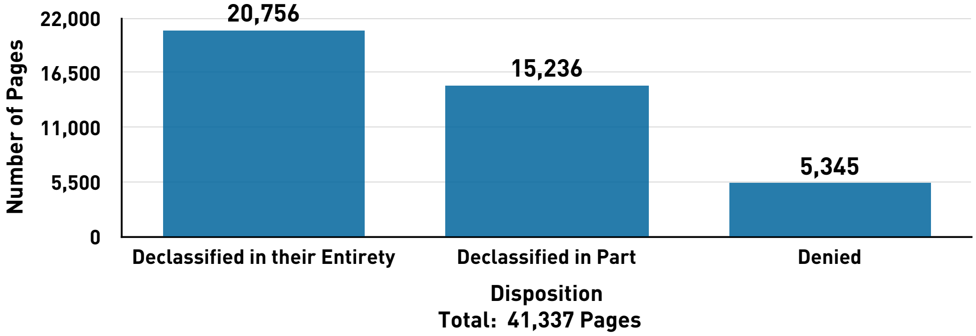
Disposition of MDR Requests FY 2014



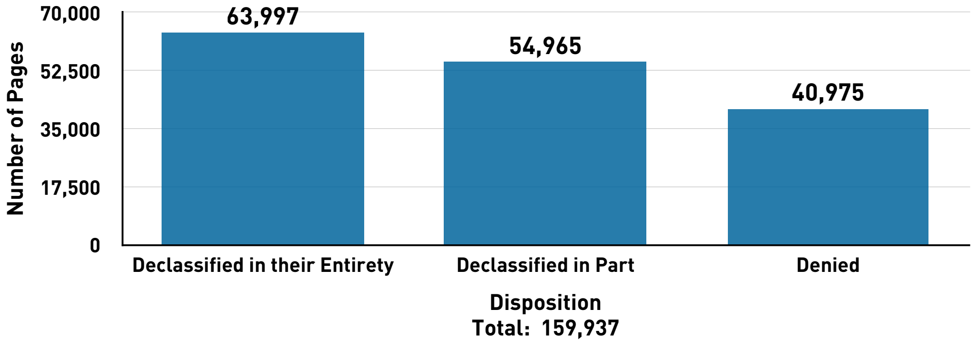
Disposition of MDR Requests FY 1996–FY 2014



Disposition of MDR Appeals FY 2014



Disposition of MDR Appeals FY 1996–FY 2014



Declassification Assessments

In FY 2014, 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, accomplishing its strategic goal of improving the quality of agency automatic declassification review programs. Overall, agencies have improved the quality of agency automatic declassification reviews since FY 2008, when ISOO began this oversight program.

Starting in FY 2013, ISOO modified its declassification assessment program to monitor agencies' progress in performance. Under this approach, ISOO monitored agency automatic declassification review programs to ensure that they performed up to standards. ISOO designed the updated program to balance the 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.

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 biannual data requests to a single annual request. ISOO will only assess records reviewed by the selected agency within the previous 12 months.

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 assesses on an annual basis at least 25 percent of agencies that review a significant volume of records for automatic declassification. Beginning in FY 2013, ISOO assessed agencies identified as having a significant automatic declassification review program at least once during the four-year period. Under this program, ISOO assessed five agencies in FY 2013 and five agencies in FY 2014.

ISOO also revised the scoring criteria for FY 2013–2016 to reflect stakeholder input and results from the assessments themselves. ISOO continues to focus 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.

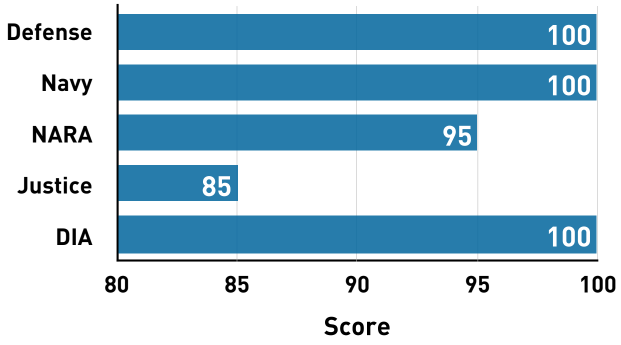
ISOO bases the overall agency score for the assessment on the occurrence and extent of any of these three issues. In addition to these three main categories, ISOO verifies that agency declassification policies and practices comply with ISOO policy guidance and that they are designed and implemented appropriately to assist the NDC in processing 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 2014: the Defense Intelligence Agency, the Department of

Justice, the National Archives and Records Administration, the Department of the Navy, and the Office of the Secretary of Defense. All five agencies received "high" scores. There were far fewer instances of missed equities, improper exemptions, and improper referrals than in previous years. ISOO did not identify any instances of missed equities or improper exemptions and only documented two instances of improper referrals. Additionally, ISOO continues to note positive progress in policy and program implementation. ISOO found that all agencies used box summary sheets and had effective record-keeping practices to document their review decisions. ISOO noted that all agencies assessed fully and appropriately used the SF 715. These practices facilitate the processing of referrals at the National Declassification Center.

In FY 2015, 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 2014



Declassification Assessment Results FY 2008–FY 2014

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
2014	5	96

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.

The senior agency official (SAO) is responsible for directing and administering the agency's self-inspection program. In order for SAOs to fulfill their responsibilities, agency self-inspection programs must be structured to provide the SAOs with information to assess the effectiveness of their agencies' classified national security information (CNSI) programs. 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 the agency self-inspection reports to 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 E.O. 13526, the reports must also answer questions relating to areas such as training, performance evaluations, and classification challenges.

In this, the fourth year of required descriptive self-inspection reporting, agency self-inspection reports generally have continued to improve. Many agencies have refined their program descriptions and appear to have made improvements to their self-inspection programs. For a number of agencies, the reports suggest that a strong and effective self-inspection program is in place, while a few agencies remain at the other end of the spectrum with reports that suggest their self-inspection programs may not be getting the attention they require. Overall, agencies are providing responses in nearly all of the required areas. However, the area of corrective actions is a concern because 15.5 percent of agencies outlined no corrective actions even though they reported deficiencies, and an additional 24.4 percent of them outlined corrective actions for some but not all of the deficiencies they reported. This means that nearly 40 percent of the agencies do not appear to be taking steps to correct some or all of the program weaknesses they identified. Many of the reported deficiencies for which no corrective actions were provided are in the key areas of training, performance evaluations, and classification challenges.

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(d)(1))

- 91.30 percent of the agencies reported that all of their cleared personnel received this training (a slight improvement over the 86.96 that reported full compliance last year).
- Although full compliance is expected, we also consider if agencies come close to meeting this requirement: 95.65 percent of the agencies report at least 90 percent compliance this year.

Refresher Training. Agencies are required to provide annual refresher training to all employees who create, process, or handle classified information. (32 CFR 2001.70(d)(4))

- 50 percent of the agencies reported that 100 percent of their cleared personnel received this training. (47.83 percent also reported full compliance last year.)
- 76.09 percent of the agencies reported at least 90 percent compliance this year.

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(d)(2))

- 50.0 percent of the agencies reported that 100 percent of their OCAs received this training (54.55 percent reported full compliance last year.)
- 63.64 percent of the agencies reported at least 90 percent compliance this year.

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)(3))

- 63.89 percent of the agencies reported that 100 percent of their derivative classifiers received this training. (61.11 percent also reported full compliance last year.)
- 80.56 percent of the agencies reported at least 90 percent compliance this year.

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))

- 36.96 percent of the agencies report that 100 percent of the required personnel have this element. (30.43 percent reported full compliance last year.)
- 47.83 percent of the agencies reported at least 90 percent compliance this year.

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))

- 80 percent of the agencies with OCA reported that delegations are limited as required. (85 percent reported full compliance last year.)

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))

- 67.39 percent of the agencies reported that they have established classification challenge procedures. (71.74 percent reported full compliance last year.)

Agencies also reported on 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 287,446 documents were reviewed to evaluate the application of this requirement. (A considerable increase from the 35,503 last year.)
- Agencies reported that 71.42 percent of the documents meet this requirement (a slight decrease from 73.36 percent last year).

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 179,650 documents were reviewed to evaluate the application of this requirement. (A considerable increase from the 30,035 last year.)
- Agencies reported that 66.86 percent of the documents meet this requirement (a decrease from 74.84 percent last year).

The low level of compliance with these core CNSI program requirements is troubling, particularly in the area of performance plans covering the designation and management of classified information. It is also a significant concern that some agencies have identified deficiencies in these areas but have not outlined actions to correct them. ISOO will emphasize to agencies that it is essential to address these shortcomings and will follow up on these issues during on-site reviews.

Overall, however, we remain cautiously optimistic that the increased emphasis on self-inspections under E.O. 13526 is having a positive effect on agency CNSI programs. We have seen improvements in the reports from many agencies over the past four years, which likely translate into improvements in the agencies' self-inspection and CNSI programs. Some agencies take their self-inspections very seriously and submit thoughtful reports that describe well-conceived and effectively implemented self-inspection programs and that report findings frankly with careful analysis and sound steps to remedy deficiencies. A number of agencies have identified best practices that others may find useful for their own CNSI programs, for example:

- Pop-up reminders of required training on system log-in that restrict system access if training is not completed as required.
- Working with ISOO, an agency modified the Standard Form 715, "Declassification Review Tab," for use electronically. By using this form in electronic format, the agency has aligned its business process requirements and improved the efficiency of its declassification review program.
- Codes added to documents that are printed from high-side systems to identify who printed them.
- Centralized quality-control for self-inspection document reviews.
- A list of personnel who are granted unescorted access to the Sensitive Compartmented Information Facility (SCIF) is posted at the door of the SCIF in an office with a high turnover of cleared personnel.
- Dual-layered process to check inspection results from front-line security managers.
- Review of clearance holders' continuing need for access over a three year period, and
- Director of Security partnership with Bureau senior leadership to emphasize a top-down approach to achieving security compliance.

We look forward to continuing to work with agencies to help them improve their self-inspection programs and to learn from the agencies that have effective programs. The value of self-inspection programs in evaluating CNSI programs to identify strengths and weaknesses and effect improvements cannot be underestimated. The investment of resources in self-inspections yields tangible results, leading to more effective, more reliable CNSI programs.

ON-SITE REVIEWS

General Program Reviews

In FY 2014, pursuant to sections 5.2(b)(2) and (4) of E.O. 13526, ISOO conducted seven on-site reviews of Executive branch agencies to evaluate the agencies' implementation of the classified national security information program. The reviews covered core program elements, such as program organization and management, classification and marking, security education and training, self-inspections, security violation procedures, safeguarding practices, and information systems security. The agencies were chosen this year because information obtained from sources such as the agencies' self-inspection reports or the report of the evaluation conducted by the agencies' Inspectors General under the Reducing Over-Classification Act indicated there may be elements of the agencies' classified national security information programs that need improvement. We also considered the size and scope of each agency's program as a factor in our selection process. The following paragraphs outline issues that were identified at multiple agencies during on-site reviews this year.

Fundamental program organization and management requirements are not being met at several of the agencies ISOO reviewed. Four of the agencies have not completed the process for promulgating current regulations to implement the executive order, as required by section 5.4(d0(s) of E.O. 13526, despite the passage of more than four years since E.O. was issued in 2009. Agency implementing regulations are important because they provide comprehensive, agency-specific guidance that informs and enables employees to efficiently adhere to essential program requirements. Five agencies did not meet the requirement of section 5.4(d)(7) of E.O. 13526 to ensure that the performance contract or other system used to rate civilian or military personnel performance include the management of classified information as a critical element or item to be evaluated in the rating of Original Classification Authorities (OCA), security managers or security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings.

In the area of classification management, the reviews found deficiencies in agency security classification guides and in the marking of classified documents. Security classification guides at two agencies lacked necessary data elements and supporting information that would allow someone to derivatively classify information. Each guide must, at a minimum, identify its subject matter; identify the OCA responsible for it; identify a point of contact; provide a date of issuance or last review; state precisely the elements of information to be protected; state which classification level applies to each element of information; state special handling caveats, when applicable; state a concise reason for classification; and prescribe a specific date or event of declassification. Without this information, a guide will not be effective in facilitating the proper and uniform derivative classification of information.

ISOO reviewed a total of 1,105 documents at the 7 agencies and identified marking discrepancies in 652 documents (59 percent), finding a total of 1,660 errors. At 2 of the agencies, more than 90 percent of the documents contained discrepancies, and the 329 documents reviewed between these agencies accounted for 839 of the errors. On the other end of the spectrum, 2 agencies had discrepancies in 22.35 percent and 31.2 percent of the documents, respectively. A high rate of marking discrepancies is more than just an administrative concern. The proper marking of classified materials is essential to demonstrate that information has been properly classified, to identify the individual who performed the classification action, and to communicate the period of time for which the information must be protected in the interest of national security. Proper marking also helps ensure that classified information is protected, and it is necessary for the appropriate sharing of information. Agencies can and must take steps to improve the marking of classified documents. These may include improved and targeted training, more effective use of the reviews of classified documents that E.O. 13526 requires in agency self-inspection programs, accurate and comprehensive marking tools and templates, and the use of quality control processes. To help address the problem of improper makings, ISOO has posted additional training aids on its website that focus on the fundamentals of marking classified documents.

Several agencies did not meet the security education and training requirements of E.O. 13526 and its implementing directive, 32 CFR Part 2001. Three of the agencies were not providing training, which is required by 32 CFR 2001.71(d), for persons who apply derivative classification markings. ISOO advised the agencies that this shortcoming required immediate attention. Two agencies did not offer specialized training for security staff or for personnel with special security duties, such as couriers. At two agencies, the annual refresher security training did not cover the elements required by 32 CFR 2001.71(f). We cannot over-emphasize the importance of security education and training to help ensure that personnel understand the classified national security program and their responsibilities under it. In addition to meeting the minimum requirements of E.O. 13526 and 32 CFR Part 2001, training must be tailored to the needs of the agency and the personnel who receive it to provide them knowledge of classification, safeguarding, and declassification in accordance with their duties.

Three of the agencies had not established self-inspection programs as required by section 5.4(d)(4) of E.O. 13526 and 32 CFR 2001.60. Another agency, although it conducts self-inspections, does not review a representative sample of its classification actions, as the executive order and implementing directive mandate. Self-inspections are the most effective means for agencies to evaluate their classified national security information programs, so that they can identify areas of concern and take action to improve them. Given the strong emphasis that E.O. 13526 places on self-inspections, it is inexcusable for agencies not to utilize this tool to maintain their programs.

ISOO is continuing to conduct on-site reviews in fiscal year 2015 and will engage with agencies that were reviewed this year to determine the degree to which they have addressed the issues that were identified during the ISOO on-site reviews. We will also engage with those other agencies that have failed or marginally applied key elements of the classified national security program as reflected in their self-inspection reporting data.

INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

Background

The President created the Interagency Security Classification Appeals Panel (ISCAP) (hereafter referred to as the Panel) by executive order in 1995 to perform the functions noted below. 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.

Mandatory Declassification Review (MDR) Appeals

During FY 2014, 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 48 MDR appeals, containing a total of 451 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 113 documents (25 percent), declassified 181 documents (40 percent) in their entirety, and declassified 157 documents (35 percent) in part.

Since May 1996, the Panel has acted on a total of 1,960 documents. Of these, the Panel declassified additional information in 71 percent of the documents. Specifically, the Panel declassified 590 documents (30 percent) in their entirety, declassified 797 documents (41 percent) in part, and fully affirmed the declassification decisions of agencies in 573 documents (29 percent).

Classification Challenge Appeals

During FY 2014, the Panel adjudicated one classification challenge appeal filed by an authorized holder of classified information, as provided for in section 1.8 of the Order. The Panel affirmed the classifying agency's original determination in this appeal.

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, approving 23 throughout FY 2012 and FY 2013. In FY 2014, the Panel authorized the Office of the Secretary of Defense and the Nuclear Regulatory Commission to exempt limited categories of information from automatic declassification at 50 years. ISOO published the updated listing of agencies eligible to exempt information at 25, 50, and 75 years as ISOO Notice 2014-04.

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 continued to add to and refine its listing of released documents during FY 2014.

ISCAP Appeals Status Log

In accordance with the spirit of the President's Open Government National Action Plan, the ISCAP staff released an appeals status log on its website in FY 2014. This log, updated quarterly, includes all appeals active during the current Presidential administration, listing the appeal number, date of request, appellant's name, source of the appeal, and the status of the appeal. The ISCAP staff also posted information about status categories and about the process of appeal prioritization for ISCAP review.

ISCAP Members*

John W. Ficklin, Chair
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

Jennifer L. Hudson
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 2014.*

Support Staff

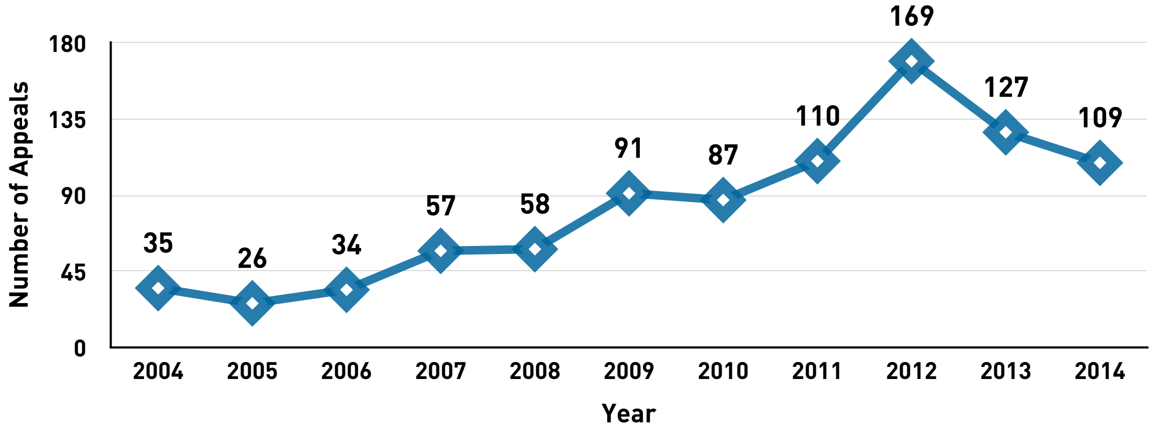
Information Security Oversight Office

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

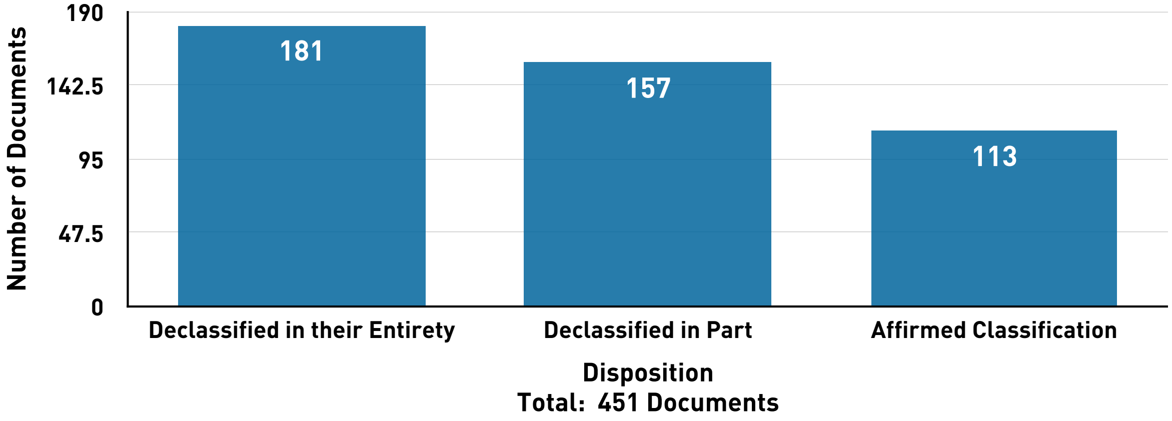
Telephone: 202.357.5250
Fax: 202.357.5908
E-mail: iscap@nara.gov

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

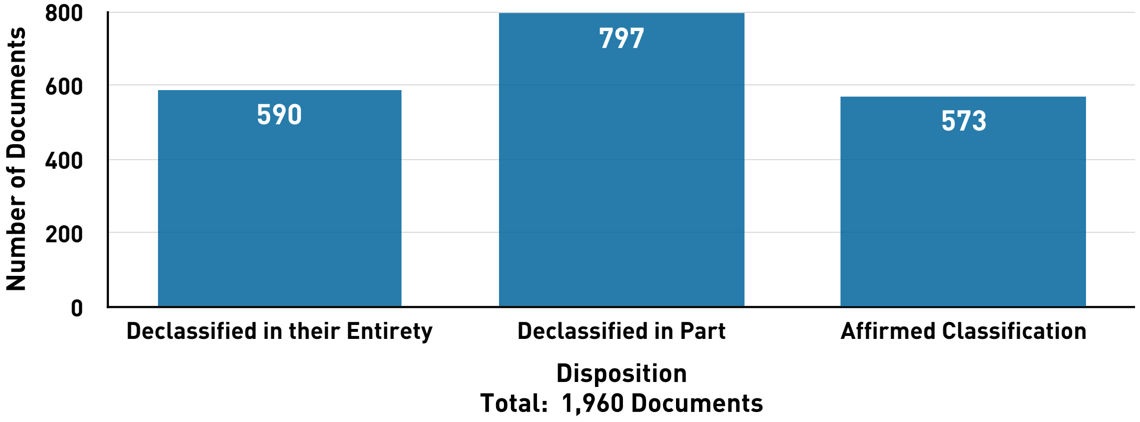
Number of Appeals Received by ISCAP
FY 2004–FY 2014



ISCAP Decisions
FY 2014



ISCAP Decisions
May 1996–September 2014



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 workforce, 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 2014 is $14.98 billion. The cost estimate of the Intelligence Community (IC)* is $1.94 billion, approximately 13 percent of the total government costs.

For FY 2014, agencies reported $1.49 billion in estimated costs associated with Personnel Security, a decrease of $22.71 million, or 1 percent.

Estimated costs associated with Physical Security were $2.20 billion, a decrease of $110.87 million, or 5 percent.

Estimated costs associated with Classification Management were $376.12 million, an increase of $22.14 million, or 6 percent.

Estimated costs associated with Declassification were $101.96 million, an increase of $2.19 million, or 2 percent.

Estimated costs associated with Protection and Maintenance for Classified Information Systems was $7.57 billion, an increase of $3.17 billion, or 72 percent, from the estimate reported for FY 2013. The main driver of this change was the report of the Department of Defense, whose estimate rose from $3.4 billion in FY 2013 to $6.6 billion for FY 2014, a net increase of $3.2 billion. ISOO and the Department of Defense worked together to better understand the nature of such a significant rise. Much was attributable to the many new initiatives underway in the aftermath of the serious security breaches that have occurred in recent years. As a result of the issuance of E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks, and the Responsible Sharing and Safeguarding of Classified Information," enhanced technical safeguarding policies for national security systems have been developed and are being phased in. These upgraded safeguards address and improve network security by reducing anonymity, enhancing access controls and user monitoring, establishing enterprise auditing, restricting the removal of media, and developing insider threat programs. None of these improvements come without considerable cost. For example, reducing anonymity on classified networked systems resulted in mandatory use of two forms of separate authentication. Developing a robust insider threat program entails the capability for continuous user activity monitoring to deter and detect anomalous behavior that may be indicative of an insider threat. In addition to newly programmed increases, the baseline data collection for these types of expenses changed within DoD over the years of interest.

Greater precision in DoD's reporting mechanisms also contributed to the rise. Improved insight into cost data led to discovery and attribution of additional information system security expenditures. In previous years, the DoD reporting of these expenses had corresponded to approximately 25 program elements directly identifiable with information system security.

For this year the funding planning figures include not only the funding in those program elements, but also an additional 40 percent drawn from other program elements not previously assessed as information system security costs, per se (e.g., those related to command and control, or information technology). With the new data in hand, which also permitted retrospective analysis, it can now be seen that this increase occurred over prior years between FY 2012 and FY 2013 and between FY 2013 and FY 2014. The combination of the increased scope of reporting and the two annual increases accounts for the near-doubling of DoD reporting in this category.

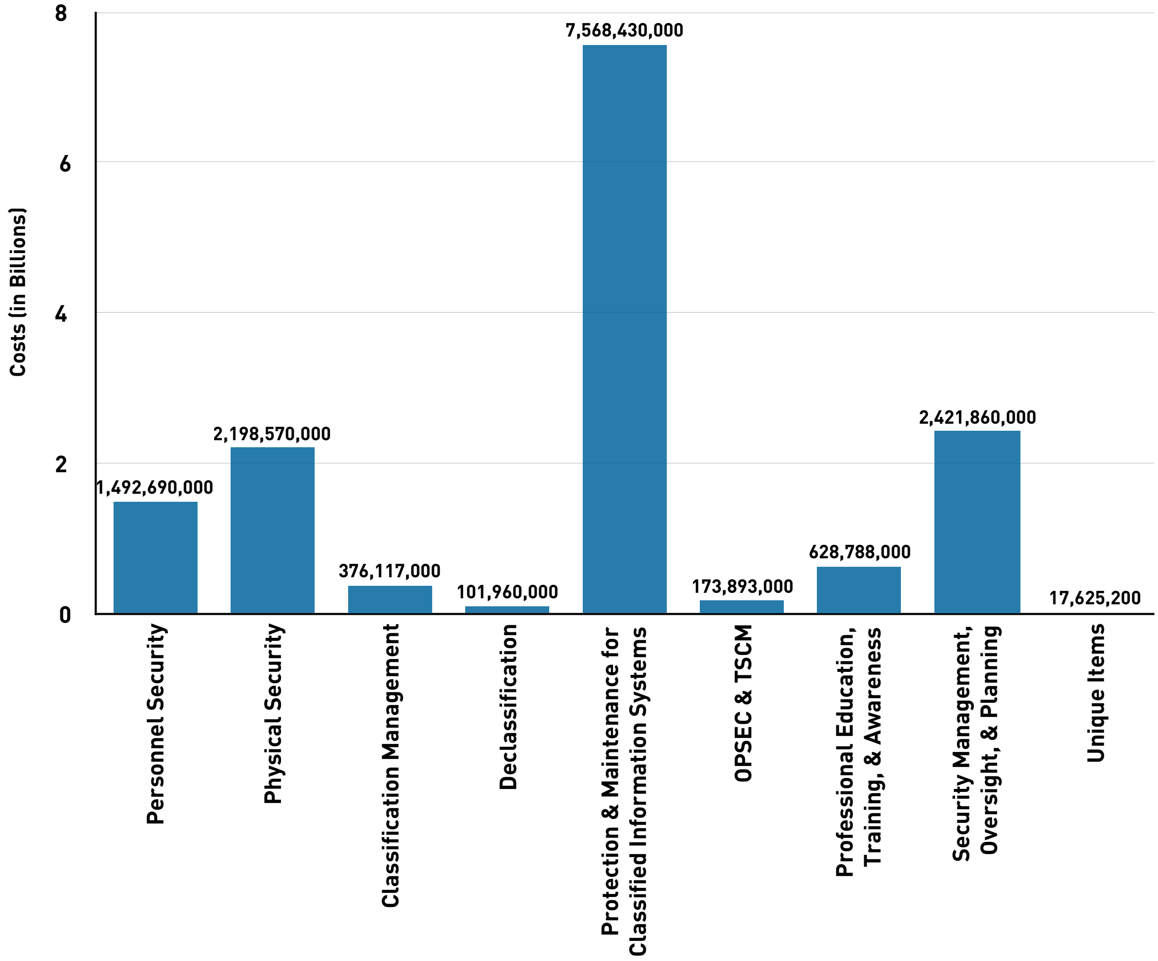
Estimated costs associated with OPSEC and TSCM were $173.90 million, a decrease of $2.94 million, or 2 percent. The estimated costs for Professional Education, Training, and Awareness were $628.78 million, an increase of $41.16 million, or 7 percent.

Estimated costs associated with Security Management, Oversight, and Planning were $2.42 billion, an increase of $250.41 million, or 12 percent. A contributor to the increased costs is the requirements for the Insider Threat program.

Estimated costs associated with Unique Items were $17.63 million, an increase of $3.95 million or 29 percent. Items in this category included the implementation and maintenance of the Registration Compliance Verification system, additional costs for COOP facilities, and costs for Nuclear Material Control and Accountability.

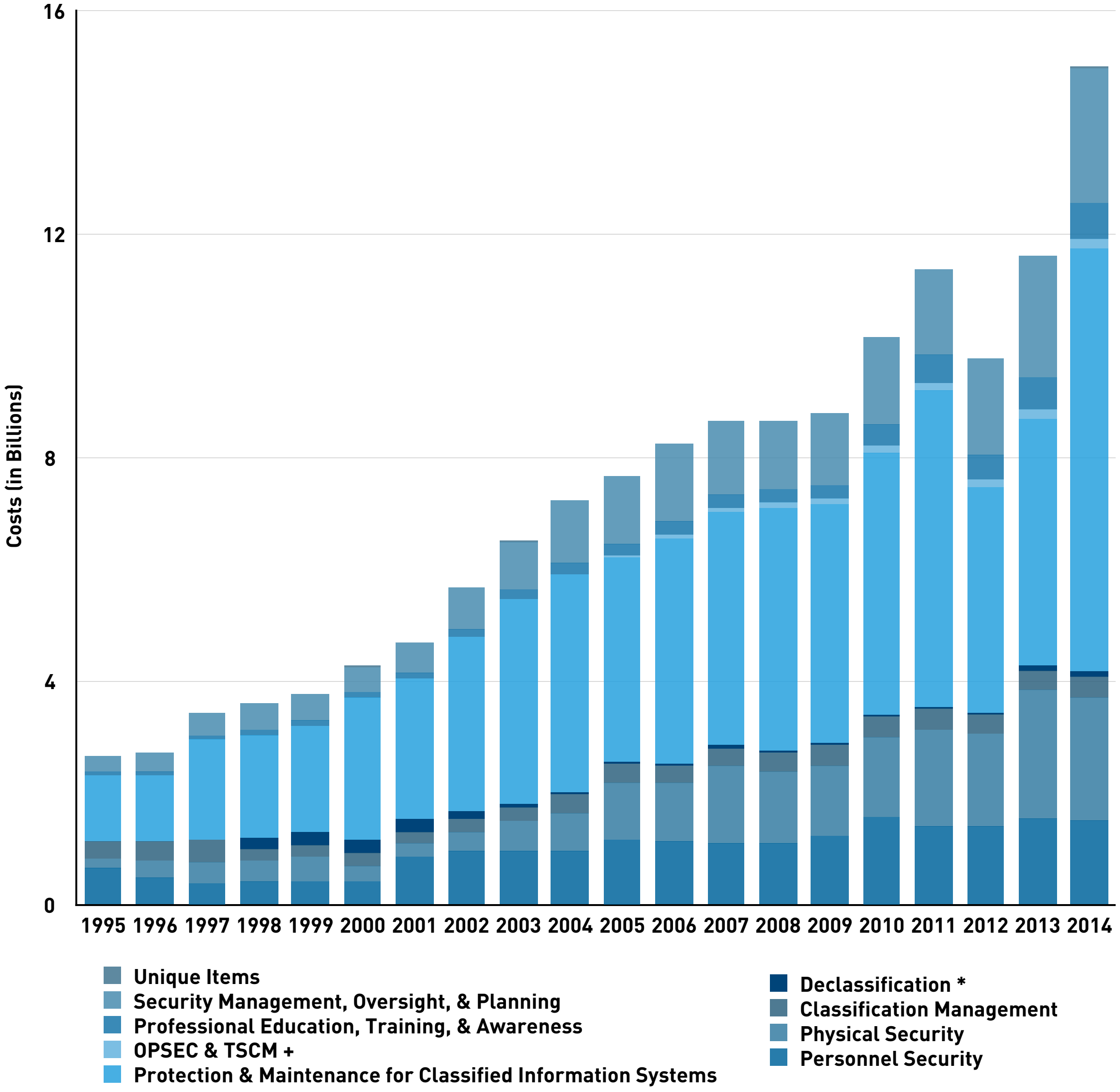
** The IC elements include the Central Intelligence Agency, the Defense Intelligence Agency, the Office of the Director of National Intelligence, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the National Security Agency*

**Government Security Classification Costs
FY 2014**



Note: Includes cost estimates from the Intelligence Community.

Government Security Classification Costs
FY 1995–FY 2014



**** 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 2014, the Defense Security Service collected industry cost data and provided the estimate to ISOO.

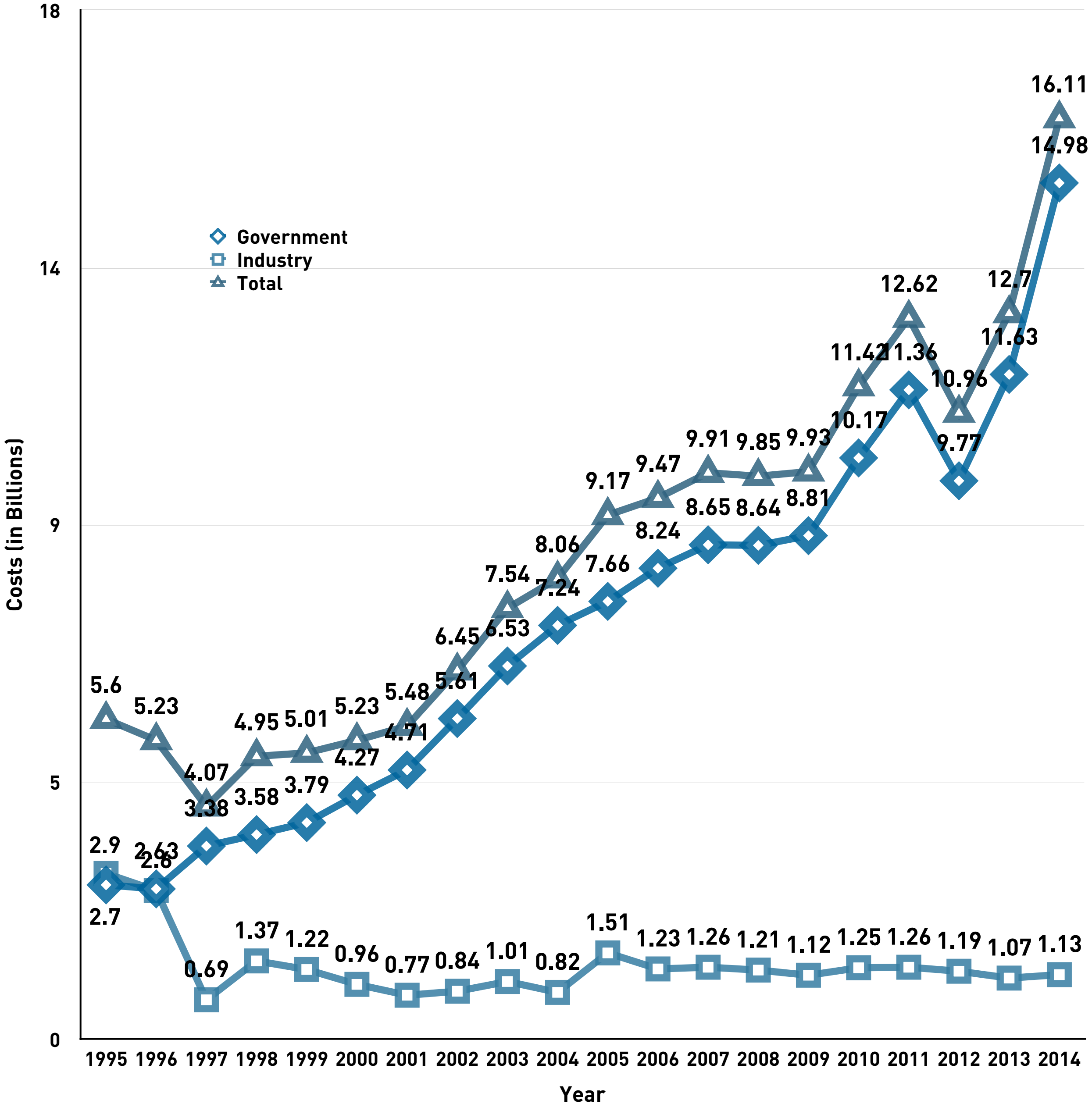
Cost-estimate data are not provided by category because industry accounts for its costs differently than Government. Rather, a sampling method was applied that included volunteer companies from four different categories of facilities. The category of facility is based on the complexity of security requirements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

The FY 2014 cost estimate totals for industry pertain to the 12-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 2014 within industry was $1.13 billion; an increase of $63.64 million, or 6 percent.

Results—Combined Government and Industry

This year's combined estimate for Government and industry was $16.11 billion, an increase of $3.42 billion, or 27 percent.

Total Costs for Government and Industry
FY 1995–FY 2014



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 2014. The major issues discussed during these 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 government policy regarding insider threat 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, was provided an opportunity to review and recommend revisions to existing guidelines and proposed changes. A conforming change that will implement insider threat in the current NISPOM will be issued in FY 2015, and a comprehensive updated NISPOM will be issued in FY 2017.

The 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 2014, we continued our outreach and support to a myriad of industrial security entities, to include: the National Classification Management Society, the Aerospace Industries Association-National Defense Intelligence Council, the American Society for Industrial Security International, and the Industrial Security Awareness Councils.

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

Background

E.O. 13556, "Controlled Unclassified Information," 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 the National Archives and Records Administration.

Following issuance of E.O. 13556, 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 initial proposed category and subcategory submissions from 47 agencies and led interagency discussions to consolidate redundancies and provide consistency among like categories. Only those categories and subcategories with a basis in law, Federal regulation or government-wide policy are authorized by the EA for designation as CUI. Categories and subcategories are defined in the CUI Registry, and are regularly reviewed and updated based on identification of unclassified information that requires protection based on law, regulations, and/or government-wide policies.

Policy Development

32 CFR Part 2002

Continuing an iterative policy development strategy of interspersed working group discussions, surveys and consolidation of current practices, initial drafting, informal agency comment, and EA comment adjudication, in June 2014, the EA submitted a proposed Federal CUI rule into the Office of Management and Budget's (OMB) formal comment process, which will be finalized as 32 CFR Part 2002. OMB's ability to reach across the Government for comment provided additional opportunity for stakeholders to submit input to CUI policy development. Using the OMB process, the EA received and adjudicated more than 800 comments from approximately 25 Executive branch agencies. The OMB process has 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). Based on input from the initial round of the OMB-managed process, procedures, definitions and protocols for appropriate safeguarding, dissemination, marking and decontrol of CUI, originally envisioned as a supplemental document, were elevated for inclusion in the proposed Federal CUI rule. The expanded draft regulation was submitted to OMB in October 2014. Under OMB supervision, this process is projected to continue in coming months, with comments to be solicited from the entire Executive branch, the private sector, and the general public.

On May 29, 2014, the ISOO Director and representatives from both Federal and non-Federal entities testified before the Subcommittee on Government Operations of the House Committee on Oversight and Government Reform regarding "Pseudo-classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information Designation." Testimony further heightened awareness of CUI policy development and underscored the mandate of E.O. 13556 that only information with a basis in law, Federal regulation or government-wide policy may be designated as CUI.

National Institute of Standards and Technology Special Publication 800-171

Section 6(a)(3) of E.O. 13556 states that "this order shall be implemented in a manner consistent with. . . applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology (NIST), and applicable policies established by the Office of Management and Budget." Therefore, 32 CFR Part 2002 will require the use of these standards and guidelines in the same way throughout the Executive branch, reducing current complexity for Federal agencies and their non-Federal information-sharing partners.

The EA has taken steps to alleviate the potential impact of the information security requirements on non-Federal organizations by collaborating with NIST to develop NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,* thus, applying information security requirements, but based in the non-Federal environment. Doing so should make it easier for non-Federal organizations to comply with the standards using the systems they already have in place, rather than trying to use government-specific approaches, when processing, storing, and transmitting CUI.

Federal Acquisition Regulation

The EA also anticipates establishing a single Federal Acquisition Regulation (FAR) clause that will apply the requirements of 32 CFR Part 2002 and NIST SP 800-171 to the contractor environment. This will further promote standardization to benefit non-Federal organizations that may struggle to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from different federal agencies for the same information creates confusion and inefficiencies. Until the formal process of establishing such a single FAR clause is complete, where necessitated by exigent circumstances, the NIST SP 800-171, when finalized, may be referenced in a contract-specific requirement on a limited basis consistent with the regulatory requirements.

Policy Development Summary

32 CFR Part 2002, NIST SP 800-171, and the CUI clause of the FAR will, in concert, provide both Federal and non-Federal organizations, including contractors, with streamlined and uniform requirements for managing CUI. Information security requirements for CUI tailored to non-Federal systems will enable non-Federal organizations to comply with statutory and regulatory requirements, and to consistently implement safeguards for the protection of CUI.

Implementation of the CUI program is being planned along a phased timeline, and will include responsibilities for both the EA and agencies. Based on stakeholder input, implementation planning workshops, and consultation with OMB, the CUI EA will develop a National Implementation Plan that will include target dates for phased implementation.

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 32 CFR Part 2002, 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.

Training

To prepare for agency-specific needs, the EA conducted an informal survey in March 2014 to gather data from affected agencies to serve as a planning aid for Executive branch-wide implementation. Data collected for training identified existing training programs and requirements, impacted personnel, target audiences, and requirements for future CUI implementation across the Executive branch. In May and September of 2014, the EA conducted specialized workshops on CUI training to collaborate with impacted agencies, discuss implementation workplan training activities, and solicit input on training deliverables including draft training learning objectives.

In preparation for EA-developed CUI training modules, the EA conducted an informal survey on agency technical training requirements in June 2014. The data served as a planning aid to assist the EA in collecting initial information on technical standards to ensure broad applicability of training development across the Executive branch. Responses were received from over 30 affected Executive branch agencies identifying a broad range of agency training requirements.

As a follow-up to the FY 2014 issuance of *Revised 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 July 2014, the EA issued an updated version of *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 developed training toolkit aids to assist agencies with CUI awareness and messaging as a lead-in to publication of 32 CFR Part 2002 and implementation of respective agency programs. Products developed include paper-based job aids, CUI implementation posters, and phased implementation charts of recommended agency-specific training activities.

Within six months of the issuance of 32 CFR Part 2002, the EA plans to issue CUI baseline training modules based on final policy and guidance. Each module will review key policy elements of the rule including safeguarding, dissemination, marking, and decontrol procedures. Training modules will meet a broad range of technical specifications and will allow for tracking within agency learning management systems.

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

Outreach and Oversight

The CUI Oversight Program is designed to assist agencies in developing, implementing, and sustaining their respective CUI programs.

In FY 2014, the EA initiated the CUI Program Appraisal process to assist Executive branch agencies in preparing for implementation of the CUI Program. The appraisal process is designed to be flexible and responsive to emerging developments and individual agency needs. A CUI Program Appraisal is scheduled based on agency request, and examines the policies, methods, and practices currently used by an agency to protect sensitive information. Key elements of focus include: safeguarding practices, program management, training/awareness, self-inspections, and incident remediation. Appraisal results provide agency planners with a baseline for developing implementation activities. In FY 2014, the EA conducted 8 appraisals; 12 appraisals are currently scheduled for FY 2015.

Standardized forms, templates, and electronic survey tools have been developed to streamline the appraisal process. An agency-completed pre-appraisal Request for Information Form is used by the EA to plan appropriate appraisal activities. A Program Baseline Form, also completed by agencies, provides a catalog of existing agency policies, procedures, methods, and practices for handling sensitive information.

To establish a complete and accurate description of current status regarding established policies, procedures, methods and practices surrounding the proper handling and protection of CUI, an online survey of 28 questions is distributed to all agency employees, contractors, and detailees.

More than 2,300 surveys were returned across the 8 appraisals conducted in FY 2014. Returns indicate that over 80 percent of respondents work in positions that require handling and protection of sensitive information, a finding that underscores the value of consistent practice. Other observations include a significantly higher response rate as awareness of the CUI Program increases across the Executive branch, and for CUI appraisals conducted independently from a scheduled ISOO inspection.

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

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.

The online CUI Registry currently includes descriptions for 22 categories and 81 subcategories of unclassified information, supported by 313 unique control citations and 106 unique sanction citations in the United States Code (U.S.C.), Code of Federal Regulations (CFR), and government-wide policies. All references were reconfirmed and updated based on annual updates to the U.S.C., CFR, and review of government-wide policy documents.

During FY 2014, the Registry was expanded to include policy and guidance documents, to identify statutes, regulations, and government-wide policies that prescribe specific safeguarding, marking, dissemination, and/or decontrol measures in the enactment language, and to provide placeholders for identified future functionalities. Search capability and a glossary of terms were added to the Registry. 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.

In addition to the online CUI Registry, an active web presence provides updates, handouts, answers to frequently asked questions, training modules, and reports. An updated portal is currently being designed to more distinctly delineate elements of the CUI program. Providing clear and readily accessible direction will promote better protection and sharing of sensitive information both internally and externally.

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

The Star Spangled Banner

NATIONAL SONG.

SONG OR DUET

with CHORUS Ad Libitum.

Pr. 25 Cnett.
Piano Arrangement - 25 .

NEW YORK
Published by WILLIAM DRESSLER, 933 Broadway.

O say can you see ~~through~~ by the dawn's early light,
What so proudly we hail'd at the twilight's last gleaming,
Whose broad stripes & bright stars through the perilous fight
O'er the ramparts we watch'd, were so gallantly streaming?
And the rocket's red glare, the bomb bursting in air,
Gave proof through the night that our flag was still there,
O say does that star-spangled banner yet wave
O'er the land of the free & the home of the brave?

On the shore dimly seen through the mists of the deep,
Where the foe's haughty host in dread silence reposes,
What is that which the breeze, o'er the towering steep,
As it fitfully blows, half conceals, half discloses?
Now it catches the gleam of the morning's first beam,
In full glory reflected now shines on the stream,
'Tis the star-spangled banner — O long may it wave
O'er the land of the free & the home of the brave!

And where is that band who so vauntingly swore,
That the havoc of war & the battle's confusion
A home & a Country should leave us no more?
— ~~[illegible]~~
Their blood has wash'd out their foul footstep's pollution
No refuge could save the hireling & slave
From the terror of flight or the gloom of the grave,
And the star-spangled banner in triumph doth wave
O'er the land of the free & the home of the brave.

O thus be it ever when freemen shall stand
Between their lov'd home & the war's desolation!
Blest with vict'ry & peace may the heav'n rescued land
Praise the power that hath made & preserv'd us a nation.
Then conquer we must, when our cause it is

INFORMATION SECURITY
OVERSIGHT OFFICE

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION

700 PENNSYLVANIA AVENUE, NW, ROOM 100
WASHINGTON, DC 20408-0001

TELEPHONE: 202.357.5250
FAX: 202.357.5907
EMAIL: *isoo@nara.gov*
www.archives.gov/isoo

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

NATIONAL
ARCHIVES