2016

REPORT TO THE PRESIDENT

NATIONAL
ARCHIVES

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

Celebrating the 100th year of the National Park Service

Front Cover: Lake McDonald at Glacier National Park, Montana. In 2016, the U.S. National Park Service celebrated the 100th anniversary of its establishment. On August 25, 1916, President Woodrow Wilson signed the legislation that created the bureau in the Department of the Interior that would manage 35 national parks and monuments that had been established since Yellowstone became the first national park in 1872.

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.
- Review requests for original classification authority from agencies.
- 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 and suggestions with respect to the administration of the programs established under the Order.
- Collect and analyze relevant statistical data and, along with other information, report them annually to the President.
- 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.
- Serve as Executive Agent to implement the Controlled Unclassified Information (CUI) program under 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.

Dear Mr. President

I am pleased to submit the Information Security Oversight Office's (ISOO) Report for Fiscal Year 2016, as required by Executive Order 13526, "Classified National Security Information" (the Order).

This report contains ISOO's analysis of the health of the Government-wide security classification system, the National Industrial Security Program (NISP) and the Controlled Unclassified Information (CUI) Program based upon data collected from executive branch agencies and departments (agencies). It also provides ISOO's evaluation of agency self-assessment reporting and the cost of security classification activity.

The data concerning derivative classification continues to be problematic for agencies to capture and ISOO to analyze accurately. Agencies estimate the number of these decisions based on established sampling methods. Although estimated, we believe this data still adds value to the overall depiction of the classification management program. First, and foremost, the data assists in identifying where agencies create, receive, and maintain classification decisions, allowing more targeted oversight and proper fund allocation. Second, an estimated count of derivative classification activity assists in identifying the costs for protecting classified information at agencies. ISOO will work to improve the methodology agencies use to make the derivative classification data estimate and will continue to report on this estimated count.

ISOO conducts on-site reviews at agencies to evaluate the implementation of the classified national security information (CNSI) program. These reviews cover core CNSI 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. ISOO conducted four on-site reviews of agencies in FY 2016. In addition, ISOO instituted a new follow-up review process this year, whereby we revisited CNSI programs to determine whether agencies took recommended corrective actions to resolve the deficiencies we found in previous on-site reviews. ISOO conducted five follow-up reviews this year, for a total of nine CNSI program reviews in FY 2016.

As part of ISOO's oversight function, we require agencies to conduct self-inspections of their CNSI programs and report their findings to ISOO each year. Agency self-inspection reports include narrative descriptions of the processes within each self-inspection program and summaries of findings, as well as data-centric responses to specific questions about core program requirements and the results of the review of the agency's classified product. Providing this data to ISOO ensures agencies evaluate their own CNSI programs annually and identify areas where they may improve processes and increase adherence to policies and the Order's policies.

Under ISOO's leadership, the NISP Policy Advisory Committee (NISPPAC) continues to advance the

> “ISOO will focus on improving our methodology in data collection and will begin planning and developing new measures for future reporting that more accurately reflect the activities of agencies managing classified and sensitive information.”

government-industry partnership. This year, ISOO began the process of updating the NISP implementing directive, 32 CFR part 2004, in order to improve and modernize guidance concerning insider threat requirements for NISP agencies, while emphasizing appropriate and timely information sharing. The amended directive will also contain additional guidance for vetting private sector entities. The NISPPAC continues to focus on the challenges concerning the personnel security clearance vetting process and the methodology for authorizing information systems to process, store, and transmit classified information.

ISOO exercises Executive Agent responsibilities for the CUI program. The CUI program aims to reform the inconsistent and conflicting patchwork of agency-specific policies, procedures, safeguarding measures, and labels used to handle sensitive unclassified information throughout the executive branch. During the past year, ISOO developed a CUI Federal regulation that promotes the protection of CUI, appropriate information sharing, and consistent safeguarding and dissemination practices. ISOO accomplished this monumental task with the assistance and support of an extensive list of stakeholders. These included the White House, the Federal agencies, State, local, Tribal, private sector, and educational entities, public-interest groups, and the public. Concurrently, ISOO partnered with the National Institute of Standards and Technology to issue an executive branch-wide cybersecurity standards document that promotes rigorous and heightened protections in the non-Federal environment. ISOO continued its outreach and oversight efforts to assist agencies and non-Federal partners in establishing their CUI program offices, and, with the Office of Management and Budget, issued target dates for phased implementation of the program.

As ISOO’s Director, I am committed to providing an annual report that benefits you and all the users of the security classification system, both inside and outside of government. As we begin our next reporting cycle, ISOO will focus on improving our methodology in data collection and will begin planning and developing new measures for future reporting that more accurately reflect the activities of agencies managing classified and sensitive information.

Respectfully,

Mark A. Bradley

MARK A. BRADLEY
Director

Big Bend National Park, Texas.
Photo courtesy of Bill Carpenter

TABLE of CONTENTS

NATIONAL PARKS

Our national parks tell distinctly American stories. Whether they inspire you to marvel at grand vistas, travel along scenic waterways and winding paths, or visit historic buildings and homes, discovery and exploration await.

Glacier Bay National Park & Preserve
Mount Rainier National Park
Marsh-Billings-Rockefeller National Historical Park
Acadia National Park
Grand Canyon National Park
Assateague Island National Seashore
San Francisco Maritime National Historical Park
Arches National Park
Theodore Roosevelt National Park
Kenilworth Park & Aquatic Gardens
Bandelier National Monument
Everglades National Park
Haleakalā National Park
Yellowstone National Park
Carlsbad Caverns National Park
Gulf Islands National Seashore
FOREVER / USA
2016

Photo courtesy of National Park Service

SUMMARY of FY 2016 Program Activity

Classification

Executive branch agencies reported 2,215 original classification authorities (OCA), an increase from 2,199 reported in FY 2015.

Agencies reported 39,240 original classification decisions, a decrease of 27 percent from last year.

Agencies reported using the ten-years-or-less declassification instruction for 30 percent of original classification decisions.

Executive branch agencies reported 55,206,368 derivative classification decisions; a 5 percent increase from FY 2015.

Declassification

Agencies received 9,580 initial mandatory declassification review (MDR) requests and closed 6,037 requests. The average number of days to resolve each request is 260. A total of 13,738 requests have remained unresolved for over one year. This number includes requests that have been carried over from prior years. Agencies reviewed 248,413 pages, and declassified 117,453 pages in their entirety, declassified 92,678 pages in part, and retained classification of 38,282 pages in their entirety.

Agencies received 373 MDR appeals and closed 303 appeals. The average number of days to resolve each appeal is 472. A total of 366 appeals have remained unresolved for over one year.

Agencies reviewed 16,390 pages on appeal, and declassified 5,788 pages in their entirety, declassified 5,633 pages in part, and retained classification of 4,969 pages in their entirety.

Under automatic declassification, agencies reviewed 96,577,037 pages and declassified 39,608,944 pages of historically valuable records.

Under systematic declassification reviews, agencies reviewed 5,374,544 pages, and declassified 4,268,784 pages.

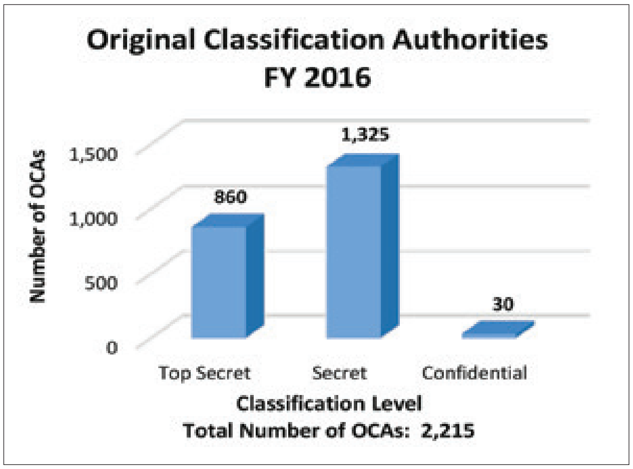
Under discretionary declassification reviews, agencies reviewed 221,122 pages, and declassified 65,872 pages.

Under automatic, systematic, and discretionary declassification reviews, a total of 102,172,703 pages were reviewed for declassification and 43,943,600 pages were declassified.

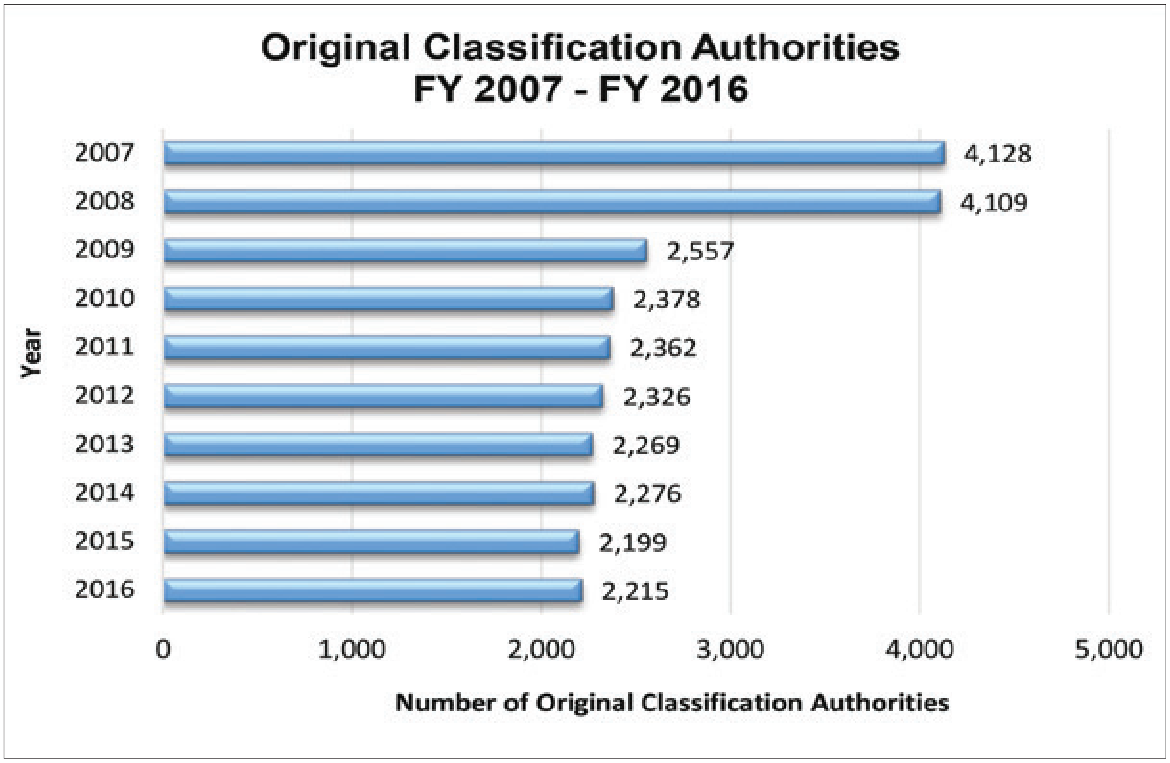
Classification

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 damage national security. Original classifiers must be able to identify or describe the damage. Agencies reported 2,215 OCAs in FY 2016; less than a 1 percent increase from the 2,199 reported in FY 2015.



"Agencies reported 2,215 OCAs in FY 2016."

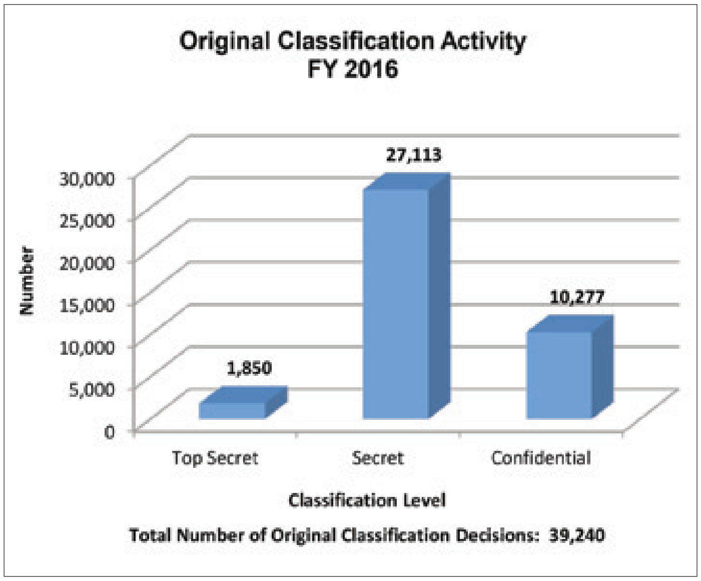


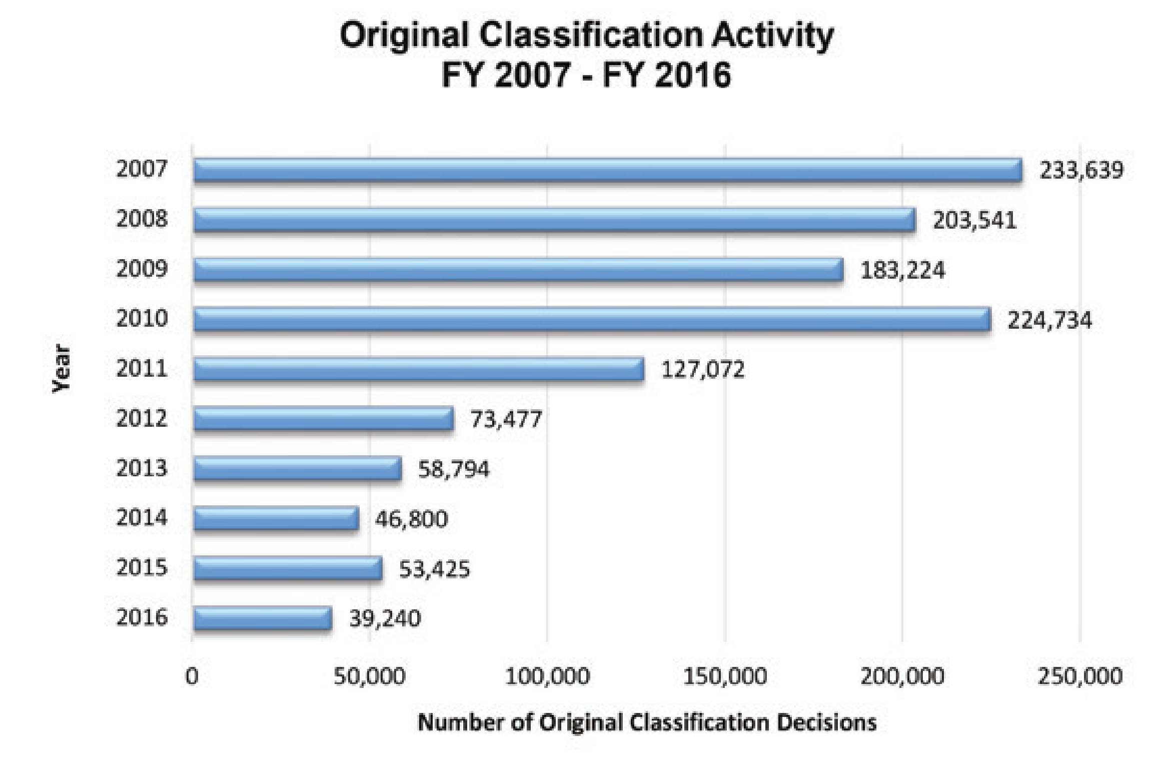
Original Classification Activity

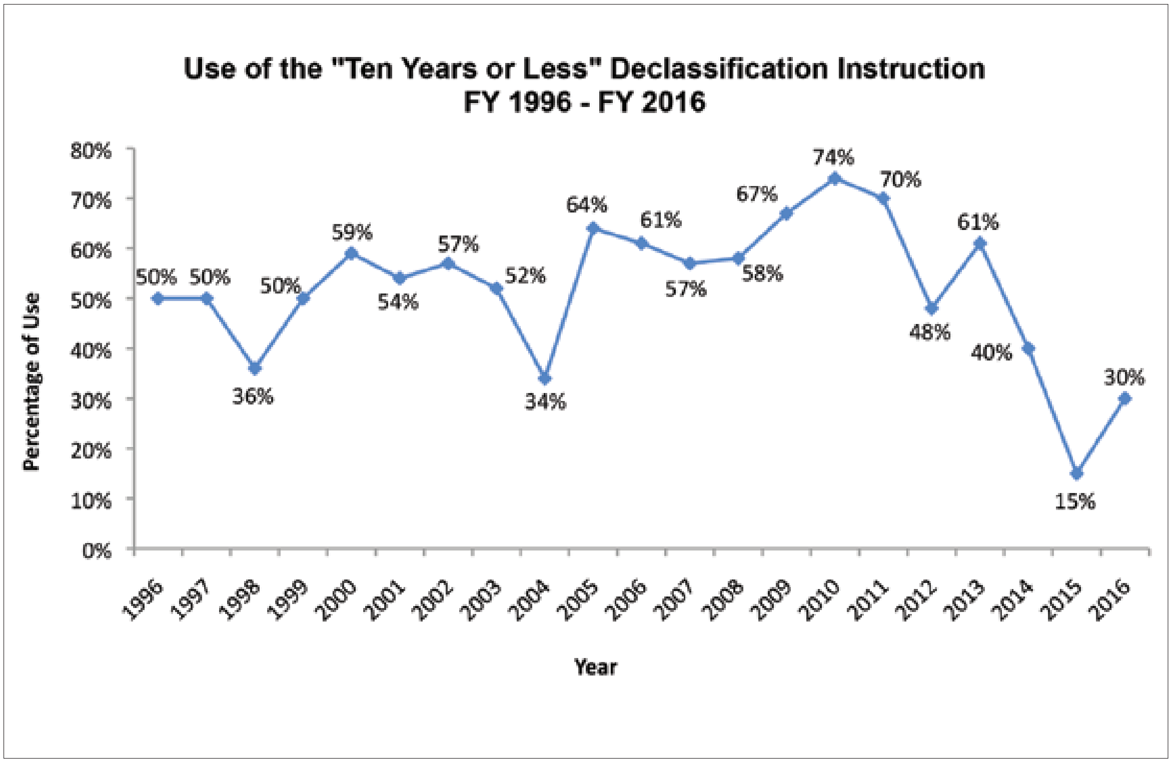
Original classification is a determination by an OCA that information owned by, produced by or for, or under the control of the U.S. Government requires protection because unauthorized disclosure of that information could reasonably be expected to damage the national security.

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.

The agencies reported 39,240 original classification decisions for FY 2016, using the ten-years-or-less declassification instruction 30 percent of the time.





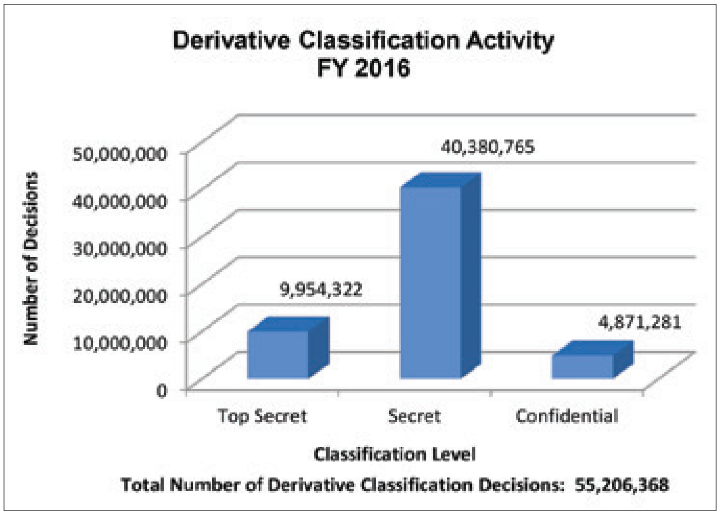


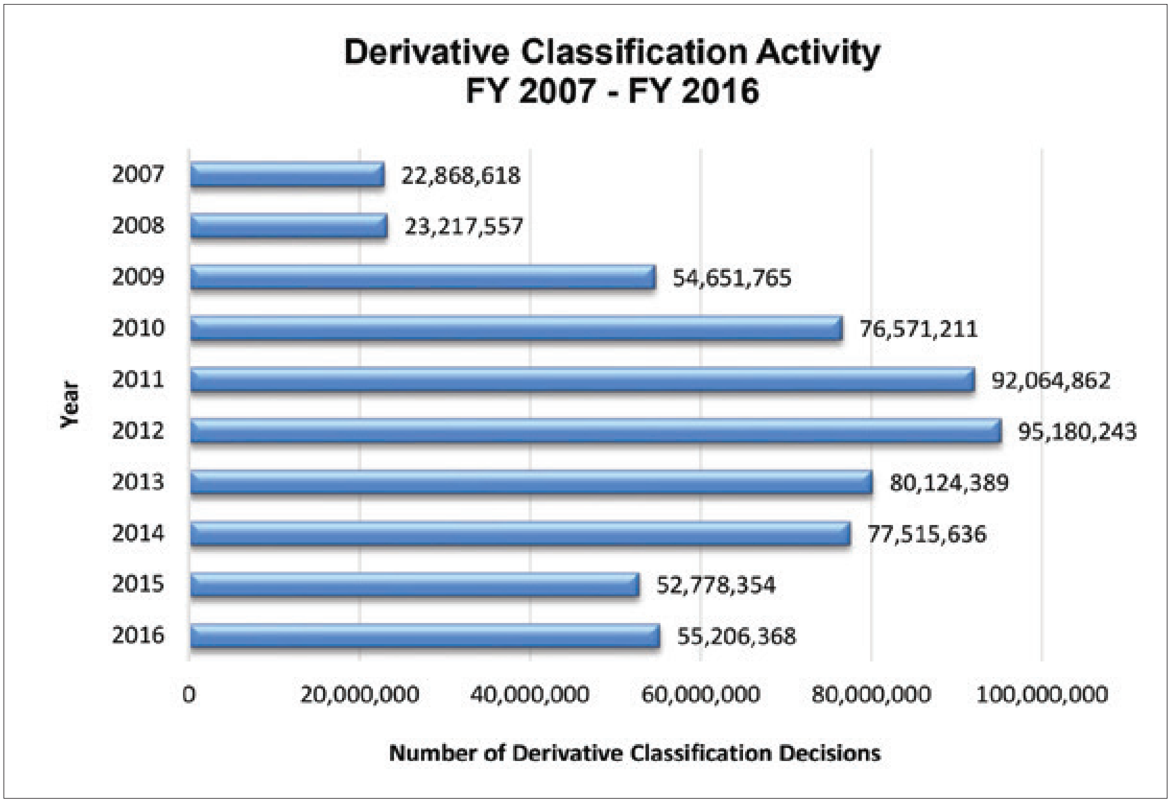
Derivative Classification Activity

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 precise elements of information regarding a specific subject that must be protected, and establishes the level and duration of classification for each such element. Classification guides provide consistency and accuracy to classification decisions.

Derivative classification actions use 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 55.21 million derivative classification decisions in FY 2016, an increase of 5 percent from FY 2015.



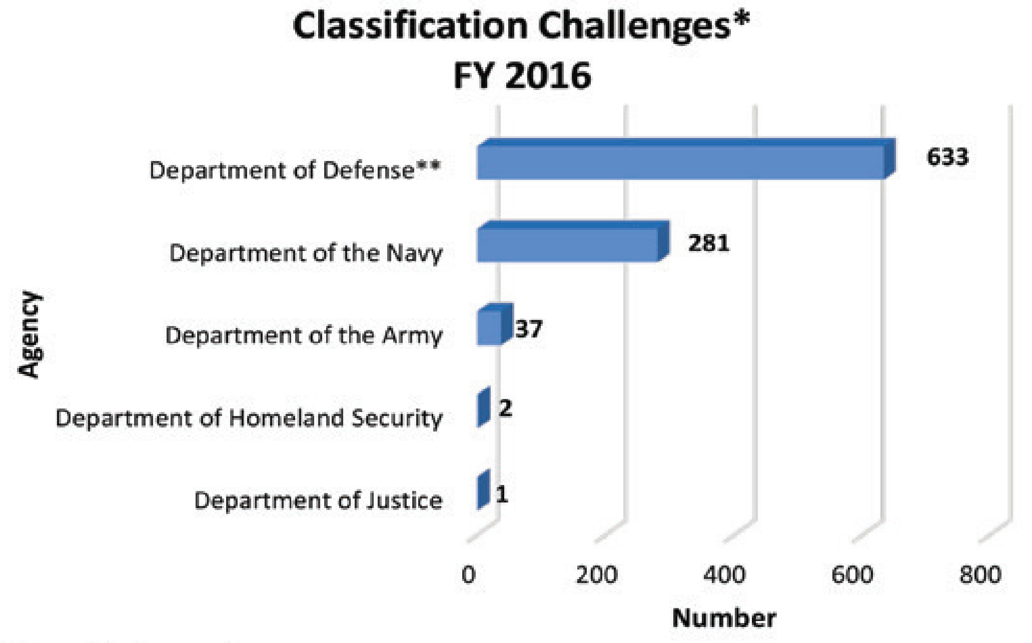


Glacier National Park, Montana. *Photo courtesy of Bill Carpenter*

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 954 formal challenges in FY 2016; 684 (71.70 percent) were fully affirmed at their current classification status with 167 (17.50 percent) being overturned either in whole or in part, and 103 (10.80 percent) challenges remaining open. The Department of Defense (DoD) historically reports the largest number of formal classification challenges, the majority of which come from the U.S. Pacific Command. This demonstrates a very solid, strong classification challenge program.



* Formal challenges only.
** OSD (1); MDA (126); NGA (1); USEUCOM (9); USPACOM (496)

> “Classification challenges provide a mechanism to promote sound classification decisions.”

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 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.

Together, these four programs are essential to the viability of the classification system and vital to an open government.

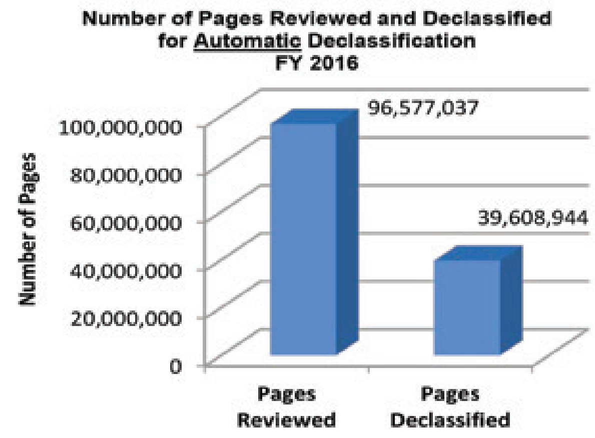
Automatic, Systematic, and Discretionary Declassification Review

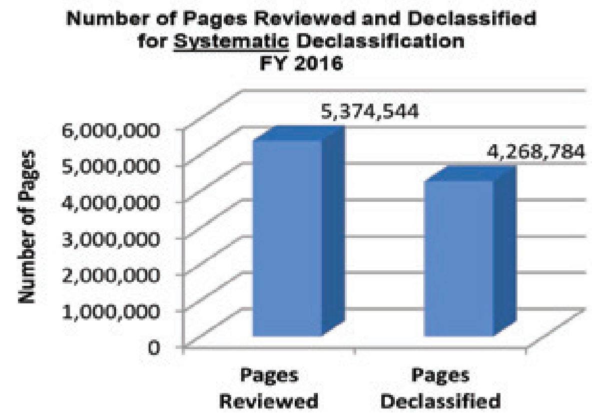
During FY 2016, a total of 102.17 million pages were reviewed under the automatic, systematic, and discretionary declassification programs and 43.94 million pages (43 percent) were declassified*. This is a 17 percent increase in the number of pages reviewed and a 19 percent increase in the number of pages declassified during FY 2015.

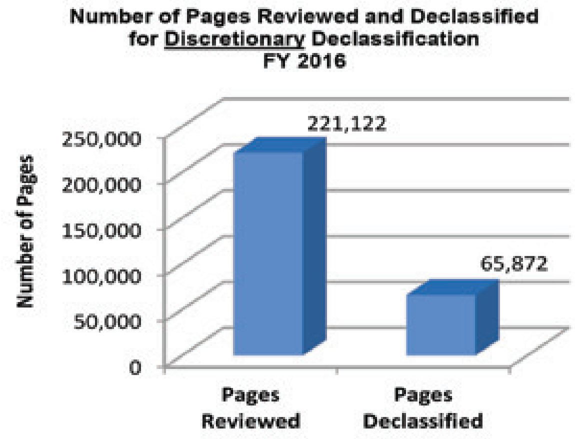
Under automatic declassification review, agencies reviewed 96.58 million pages and declassified 39.61 million pages (41 percent). Under systematic declassification review, agencies reviewed 5.37 million pages and declassified 4.27 million pages (79 percent). Under discretionary declassification review, agencies reviewed 221,122 pages and declassified 65,872 pages (30 percent).

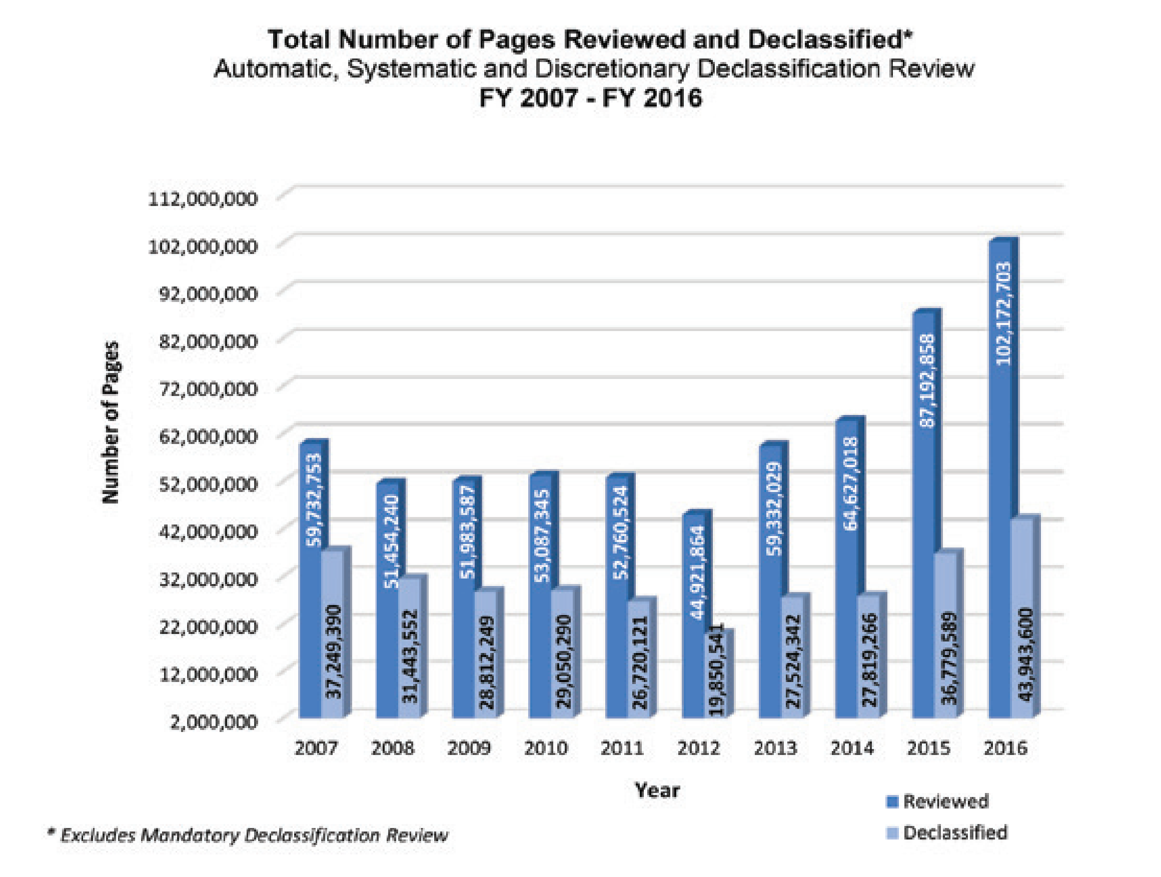
This data does not include the status of documents processed by the National Declassification Center. Information about that program can be found at* ***http://www.archives.gov/ declassification/ndc/releases.html*

Shenandoah National Park, Virginia. *Photo courtesy of National Park Service*


Number of Pages Reviewed and Declassified
for Automatic Declassification
FY 2016
Number of Pages
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
96,577,037
39,608,944
Pages Reviewed
Pages Declassified


Number of Pages Reviewed and Declassified
for Systematic Declassification
FY 2016
Number of Pages
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
5,374,544
4,268,784
Pages Reviewed
Pages Declassified


Number of Pages Reviewed and Declassified
for Discretionary Declassification
FY 2016
Number of Pages
250,000
200,000
150,000
100,000
50,000
0
221,122
65,872
Pages Reviewed
Pages Declassified



Total Number of Pages Reviewed and Declassified*
Automatic, Systematic and Discretionary Declassification Review
FY 2007 - FY 2016

** Excludes Mandatory Declassification Review*

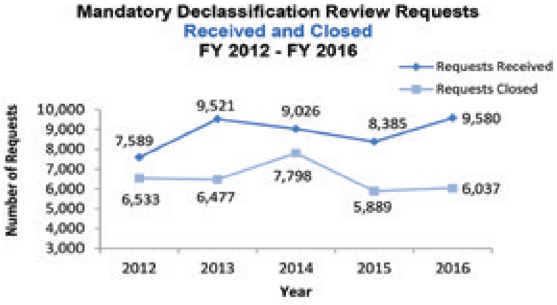
Mandatory Declassification Review

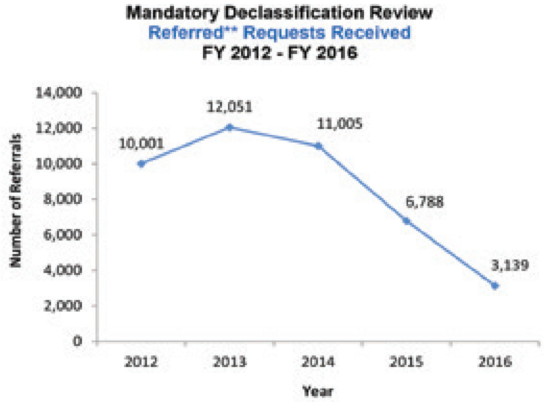
The mandatory declassification review (MDR) process requires a review of specific classified national security information in response to a request seeking its declassification. The public must make MDR requests in writing, and each request must contain sufficient specificity describing the record to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

MDR Activity, FY 2016

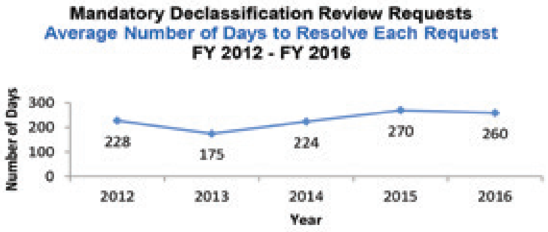
The FY 2016 data specifies the number of requests and appeals received, the number that remain unresolved for over one year, and the average number of days it takes to resolve each request and appeal. The report also displays the number of referred MDR requests and appeals to more accurately reflect the MDR workload of agencies. The number of referred MDR requests and appeals are not included in the statistical calculations to prevent duplicate counts.

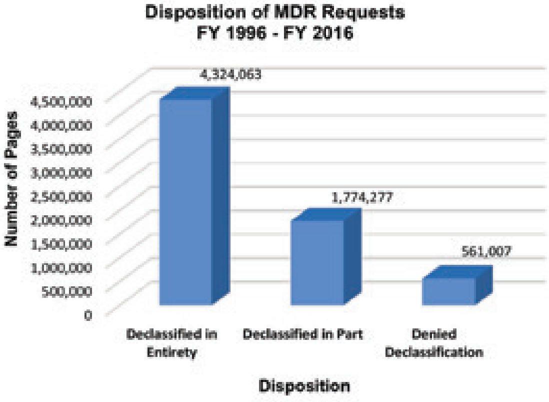
MDR Requests



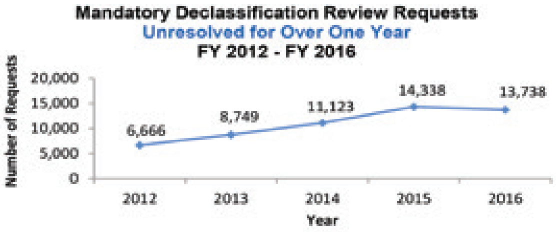


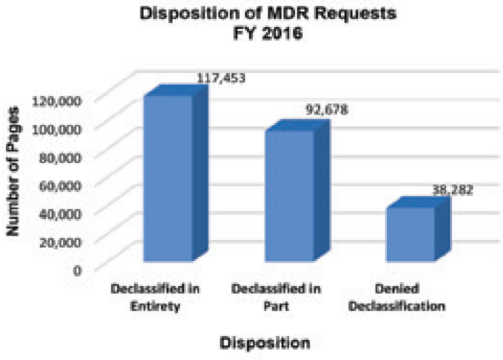
** MDRs referred to an agency from another agency that is responsible for the final release of the request.





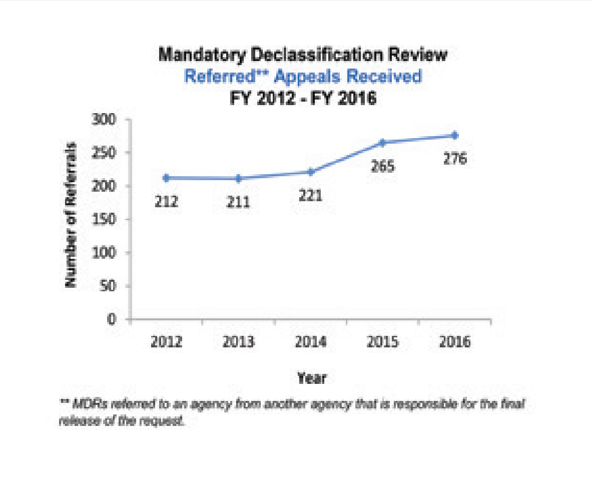
Total: 6,659,347 Pages



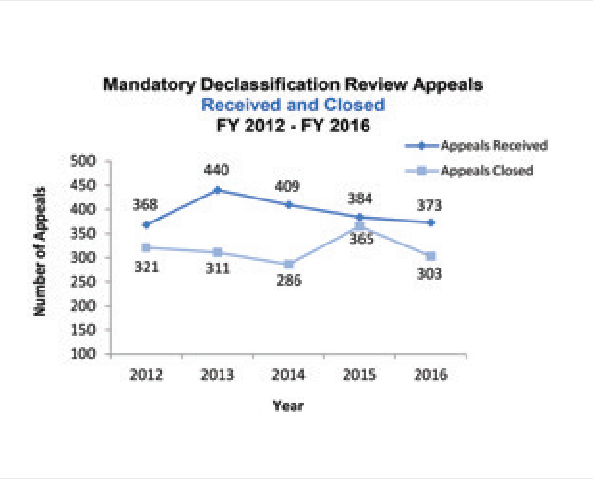


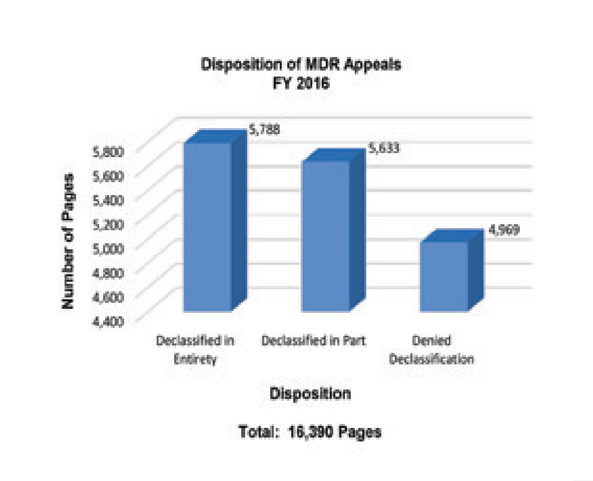
Total: 248,413 Pages

MDR Appeals

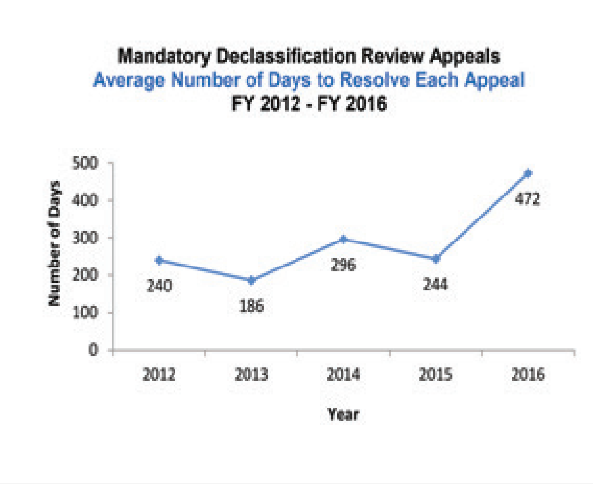

Mandatory Declassification Review
Referred** Appeals Received
FY 2012 - FY 2016

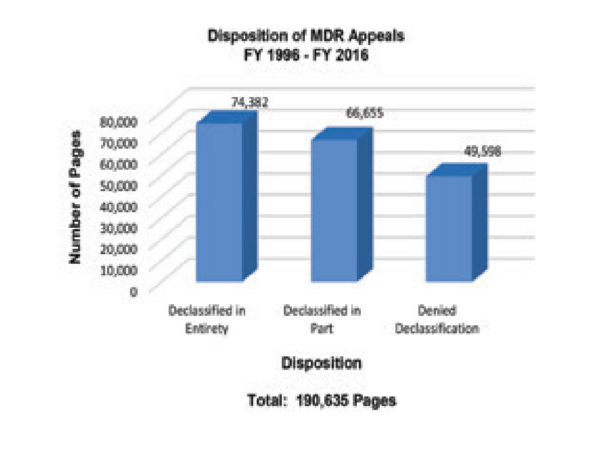
** MDRs referred to an agency from another agency that is responsible for the final release of the request.


Mandatory Declassification Review Appeals
Received and Closed
FY 2012 - FY 2016

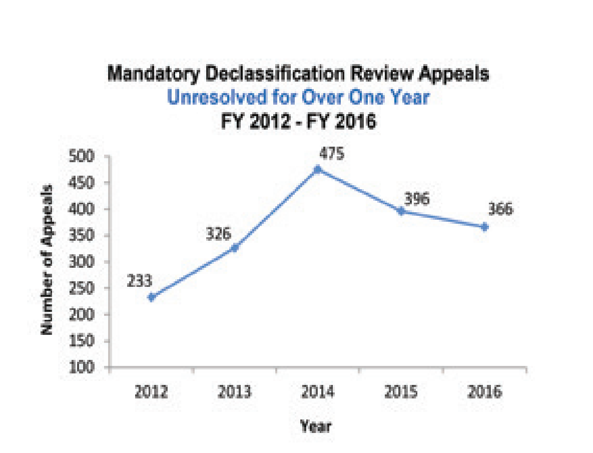

Disposition of MDR Appeals
FY 2016

Total: 16,390 Pages


Mandatory Declassification Review Appeals
Average Number of Days to Resolve Each Appeal
FY 2012 - FY 2016


Disposition of MDR Appeals
FY 1996 - FY 2016

Total: 190,635 Pages


Mandatory Declassification Review Appeals
Unresolved for Over One Year
FY 2012 - FY 2016

Reviews

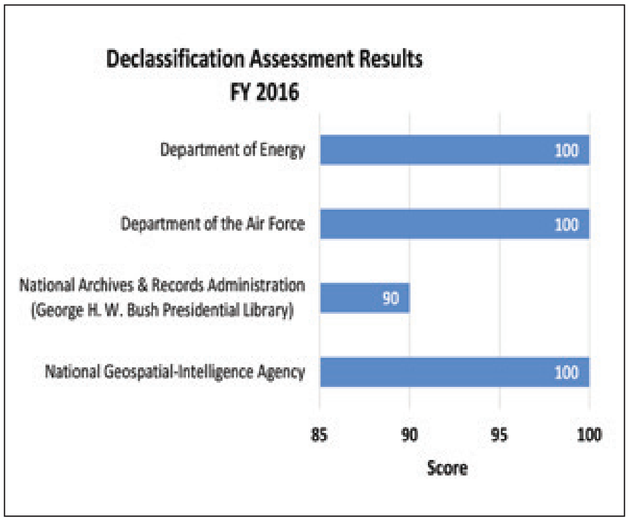
Declassification Assessments

In FY 2016, ISOO conducted declassification proficiency assessments of four agencies using an assessment plan and scoring methodology revised in FY 2013. 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.

ISOO assesses annually at least 25 percent of agencies which 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, five in FY 2014, six in FY 2015, and four in FY 2016.

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.



Declassification Assessment Results, FY 2008 – FY 2016

Fiscal Year	Number of Agencies Assessed	Average Score
2008	22	79
2009	19	84
2010	15	90
2011	15	94
2012	16	97
2013	5	91
2014	5	96
2015	6	99
2016	4	98

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 major areas of concern, ISOO verifies that agency declassification policies and practices comply with ISOO policy guidance and that they are designed and implemented appropriately to assist the National Declassification Center (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 declassification assessments of four agencies in FY 2016: the Department of Energy, the National Geospatial-Intelligence Agency, the Department of the Air Force, and the National Archives and Records Administration's George H. W. Bush Presidential Library. All four agencies received "high" scores. ISOO encountered one instance of missed equity in a record referred to another agency and two instances of improper referrals of records to an agency where referrals were not necessary. As a result of these findings, ISOO staff worked with the agency review staff to identify and eliminate the conditions that led to these findings. ISOO found that all agencies either used box summary sheets or had effective record-keeping practices to document their review decisions in the electronic environment. These practices facilitate the future processing of referrals at the NDC. Overall, ISOO continues to note positive progress in policy and program implementation.

In FY 2017, ISOO will begin a new four-year cycle of assessments in order to continue the ongoing assessment and improvement of agency declassification programs.

Self-Inspection Programs

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 them 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 used; and (2) information gathered through the agency's

Yosemite National Park. *Photo courtesy of Evan Coren*

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.

This is the sixth year of required descriptive self-inspection reporting. Self-inspection reports must include findings from the agency self-inspection programs in two ways: in narrative responses, which give agencies latitude in providing a summary and assessment that is specific to their CNSI programs, and in data-centric responses to specific questions about core CNSI program requirements that apply to all agencies. These questions relate to training, performance evaluations, delegations of original classification authority, classification challenge procedures, the marking of classified documents, and industrial security programs.

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))
  - o 91.30 percent of the agencies reported that all of their cleared personnel received this training (an increase from the 84.78 percent that reported full compliance last year).
  - o 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 (the same as last 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))
  - o 52.17 percent of the agencies reported that 100 percent of their cleared personnel received this training (the same as last year).
  - o 78.26 percent of the agencies reported at least 90 percent compliance this year (a decline from 82.61 percent from last 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))
  - o 68.18 percent of the agencies reported that 100 percent of their OCAs received this training (an improvement from the 63.64 percent that reported full compliance last year).
  - o 77.27 percent of the agencies reported at least 90 percent compliance this year (an improvement from 72.73 percent from last 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))
  - o 78.05 percent of the agencies reported that 100 percent of their derivative classifiers received this training (an improvement from the 70 percent that reported full compliance last year).
  - o 87.50 percent of the agencies reported at least 90 percent compliance this year (the same as last 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 or item to be evaluated relating to designation and management of classified information. (E.O. 13526, Sec. 5.4(d)(7))
  - o 39.13 percent of the agencies report that 100 percent of the required personnel have this element (41.30 percent reported full compliance last year).
  - o 43.48 percent of the agencies reported at least 90 percent compliance this year (compared to 50 percent last year).

> It is problematic that the level of compliance with this important requirement has fallen from an already unacceptably low level last year. Personnel must be held accountable for their work with classified information, and that a majority of the agencies do not have a satisfactory level of compliance with the performance element requirement is cause for concern. The significance of this is compounded because some agencies that identified that they do not sufficiently meet this requirement have not reported they were taking actions to correct this shortcoming.

Agencies also reported on whether they met 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))
  - 94.10 percent of the agencies with OCA reported that delegations are limited as required (90.00 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))
  - 76.09 percent of the agencies reported that they have established classification challenge procedures (76.09 percent also reported full compliance last year).

In addition, agencies 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 89,250 documents were reviewed to evaluate the application of this requirement (a decrease from the 95,394 last year).
  - Agencies reported that 76.77 percent of the documents meet this requirement (virtually the same as the 76.78 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 82,882 documents were reviewed to evaluate the application of this requirement (a decrease from the 85,685 last year).
  - Agencies reported that 70.90 percent of the documents meet this requirement (an increase from 68.98 percent last year).

Assateague Island National Seashore, Maryland and Virginia. *Photo courtesy of Bob Skwirot*

It is good that there were improvements again this year in most of the areas outlined above. However, many agencies have not reached an acceptable level of compliance in these areas. Of particular concern is that many agencies are not reporting any actions to correct deficiencies that they identify in their reports. More than 26 percent of the agencies did not outline any corrective actions even though they reported deficiencies in their narrative and/or data-centric responses, and an additional 21.70 percent of them outlined corrective actions for some but not all of the deficiencies they reported. In total, 47.80 percent of the agencies do not report that they are taking steps to correct all the program weaknesses they identified. The most frequently reported deficiency for which no corrective action was provided is, as it was last year, the failure to sufficiently meet the requirement for a performance element or item on the designation and management of classified information. For this and all deficiencies identified during self-inspection, it is imperative that all agencies use what they learn about their CNSI programs to manage and improve those programs. Agency self-inspections are an investment in the CNSI programs that can pay great dividends if the agencies utilize what is found during self-inspections. To not take corrective action is to squander the investment. In FY 2018, ISOO intends to place special emphasis on working with the aforementioned agencies to improve their information security programs.

Viewed from another perspective, though, the current status of agency self-inspection programs is positive. Ten to fifteen years ago, many agencies were not conducting self-inspections. At that time, ISOO on-site reviews found that a third of the agencies it reviewed had no self-inspection programs and a third had very

Acadia National Park, Maine. *Photo courtesy of Bob Skwirot*

weak self-inspection programs. Although a small number of agency self-inspection programs are marginal, all of the agencies now report that they have self-inspection programs, some of which are very strong and are utilized to help ensure that the CNSI program is effectively implemented.

Classified National Security Information (CNSI) Program Reviews (On-Site Reviews)

Pursuant to sections 5.2(b)(2) and (4) of E.O. 13526, ISOO conducts on-site reviews of executive branch agencies to evaluate the agencies' implementation of the CNSI program. These reviews cover core CNSI 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 reviews include a review of a sample of approximately 200 classified documents created by the agency in the two years before the review. ISOO conducted four of these full on-site reviews of executive branch agencies in FY 2016. In addition, during this period, ISOO instituted a follow-up review process, whereby agencies that were subject to an on-site review two years prior, are revisited for an evaluation of the actions that the agency took to correct the deficiencies that were identified in the earlier review. The follow-up reviews include a review of a sample of approximately 50 documents that were created by the agency in the year prior to the review. ISOO conducted five follow-up reviews in FY 2016, for a total of nine CNSI program reviews this year.

The four agencies where full program reviews were conducted all had fairly strong CNSI programs, although each had several areas where improvements were needed. In the five follow-up reviews, ISOO found that approximately half of the findings from the FY 2014 reviews had been satisfactorily addressed. The following paragraphs outline issues that were identified during on-site reviews this year. Agencies that have not been evaluated by ISOO recently should consider if their programs exhibit any of the deficiencies noted here.

In the area of program management, several of the agencies where full program reviews were conducted did not meet all of the requirements with regard to performance evaluations. Section 5.4(d)(7) of E.O. 13526 requires agencies to ensure that the performance contract or other system used to rate civilian or military personnel performance includes the designation and 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. At one agency, only two percent of the required personnel had the rating element. At two agencies, the performance plans covered only the management of classified information, not its designation. "Designation" was explicitly spelled out when E.O. 13526 was issued in December 2009 because of the importance of accurate classification and marking of classified information.

In the area of classification management, the reviews found deficiencies in agency security classification guides and in the marking of classified documents. Per 32 CFR 2001.16, agencies must review their classification guidance at least once every five years. Two agencies had guides that had not been reviewed and updated for longer than this. Per 32 CFR 2001.15(b), each classification 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. Security classification guides at two agencies lacked one or more of these elements.

ISOO reviewed a total of 752 classified documents at the four agencies during the full on-site reviews and identified marking discrepancies in 363 (48.27 percent) documents, finding a total of 550 document marking errors. The most frequently occurring type of discrepancy was the absence of some or all portion markings. The next most common error related to declassification instructions, either they were not included or they were improper or incomplete. The third most common error was the absence of a "Classified By" line or incomplete information on this line. 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 is also necessary to facilitate the appropriate sharing of information. The marking of classified documents requires constant attention through training, agency document reviews, and the use of marking tools and quality control processes. Likewise, reinforcement of the necessity for accurate marking is enhanced by ensuring the designation of classified information is included as a critical element in the performance contract or other system used to rate the performance of personnel who regularly apply derivative classification markings.

All four agencies had very good security education and training programs. Agencies are required to provide initial training, annual refresher training, training for original classification authorities and for derivative classifiers, specialized training, and termination briefings. All four agencies were providing this training. One agency, though, was delivering a double-duty training that was intended to fulfill both the refresher and derivative classification training requirements, which in itself is not problematic. However, the training did not meet the minimum requirements for either the refresher or the derivative training that are established by 32 CFR part 2001.71(d and f).

Section 5.4(d)(4) of E.O. 13526 requires agency self-inspection programs to include the regular reviews of representative samples of the agency's original and derivative classification actions. The four agencies all had sound self-inspection programs. However, two of them had identified CNSI program weaknesses during self-inspections but did not take action to correct them. One agency found that the overwhelming majority of its personnel did not have the required performance element or item covering the designation and management of classified information but did nothing to address this. Another agency identified deficiencies with the use of classification guides and the application of document markings but did not take steps to improve them.

All four agencies established sound policies, procedures, and practices to safeguard CNSI. Classified information was being protected from unauthorized access and was being appropriately communicated, transmitted, and destroyed. At one agency we did find some instances when standard security forms were not used as required. The SF 700, "Security Container Information," in one safe identified individuals who no longer worked in the office as responsible for the container. The SF 701, "Security Activity Checklist," that was in use in some offices was an outdated version that was not tailored to meet the safeguarding requirements of the specific area in which it was used. In some offices it was unclear which equipment was used to process classified information and which was used to process unclassified information because the SF 706 through 710 were not used.

For agencies that issue contracts or enter into agreements with private sector entities that require access to classified information under the National Industrial Security Program (NISP), ISOO on-site reviews cover the agencies' NISP programs in accordance with E.O. 12829 and 32 CFR part 2004. ISOO verifies the following: that the security requirements clause from the Federal Acquisition Regulation (or an equivalent, such as the Department of Energy Acquisition Regulation) has been incorporated into agency contracts requiring access to classified information, that contracts or agreements include a contract security classification specification to convey classification guidance, and that contractors are authorized for access prior to the release of classified information. ISOO also verifies that agency industrial security program personnel are provided appropriate education and training to carry out their responsibilities.

In the area of information systems security, the agencies reviewed in FY 2016 demonstrated their efforts to improve cybersecurity resilience and the ability to address the growing complexity of attacks. Overall, we found that most had established uniform procedures to ensure that automated information systems, including networks and telecommunications systems that store classified information, prevent access by unauthorized persons; ensure the integrity of the information; and to the maximum extent practicable, use common information technology standards and protocols. We also determined that requirements were addressed by deploying initiatives such as the establishment of specialized role-based information systems security training; comprehensive compliance oversight programs; privileged-user accountability systems; and network anomaly detection tools designed to track network traffic, vulnerabilities, user activity and threat intelligence in real time.

Although our review found significant efforts towards meeting requirements in support of agency-wide cybersecurity and information assurance programs, the observations and findings noted in FY 2016 revealed deficiencies in newly deployed classification management tools. At some agencies, these tools, which are intended to assist derivative classifiers in correctly classifying and marking classified information and properly marking classified electronic documents, are not fully compliant with current marking requirements. In some instances the tool was not fully implemented or users were not provided sufficient training. As a result, employees experienced difficulties using the tool when marking and sending classified emails.

With respect to policy that governs the use and control of wireless and personally owned devices, we found that the reviewed agencies have taken actions to address deficiencies. Specifically, they have implemented procedures and training on the use of portable devices. Although their efforts are a move in the right direction, many policies still lack specificity in regard to enforcement and reporting mechanisms.

As noted above, FY 2016 was the first year for follow-up reviews of CNSI programs. The follow-up reviews were prompted by a concern that agencies may not have been correcting deficiencies in their CNSI programs that ISOO found during on-site reviews. The follow-up reviews are conducted to examine only the program areas where issues were identified in the previous review and determine if an agency has satisfactorily addressed the findings and recommendations of the initial review. The concerns were not unfounded, as the five follow-up reviews found that only 46 percent of the findings and recommendations had been addressed. Two of the agencies, however, did satisfactorily address the majority of the issues—60 and 67 percent, respectively—but the other three agencies had low rates of taking corrective actions, ranging from 31 to 45 percent. The document reviews conducted during the follow-up reviews evaluated 238 documents and found that just over 60 percent of the documents contained errors. The most frequently occurring error was the absence of a "Classified By" line or incomplete information on this line. The next two most common errors were the absence of some or all portion markings and declassification instructions that were either were not included or were improper or incomplete.

The follow-up reviews did get the attention of agency leadership and prompted responses indicating that actions were being taken to address the open findings. These corrective actions will need to be validated, and we are hopeful that steps have been taken to address the deficiencies. We are also hopeful that the practice of follow-up reviews will motivate agencies to take corrective actions after the initial review because of the expectation that ISOO will return soon to their agencies to verify that such actions have been taken.

> "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 is also necessary to facilitate the appropriate sharing of information."

Interagency Security Classification Appeals Panel

Background

The President created the Interagency Security Classification Appeals Panel (ISCAP) by executive order in 1995 to act as the appellate authority for classification and declassification decisions. The ISCAP 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 Chair. The Director of the Information Security Oversight Office serves as its Executive Secretary. ISOO provides staff support to ISCAP 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 decisions on appeals under sections 1.8 and 3.5 of E.O. 13526.

Mandatory Declassification Review (MDR) Appeals

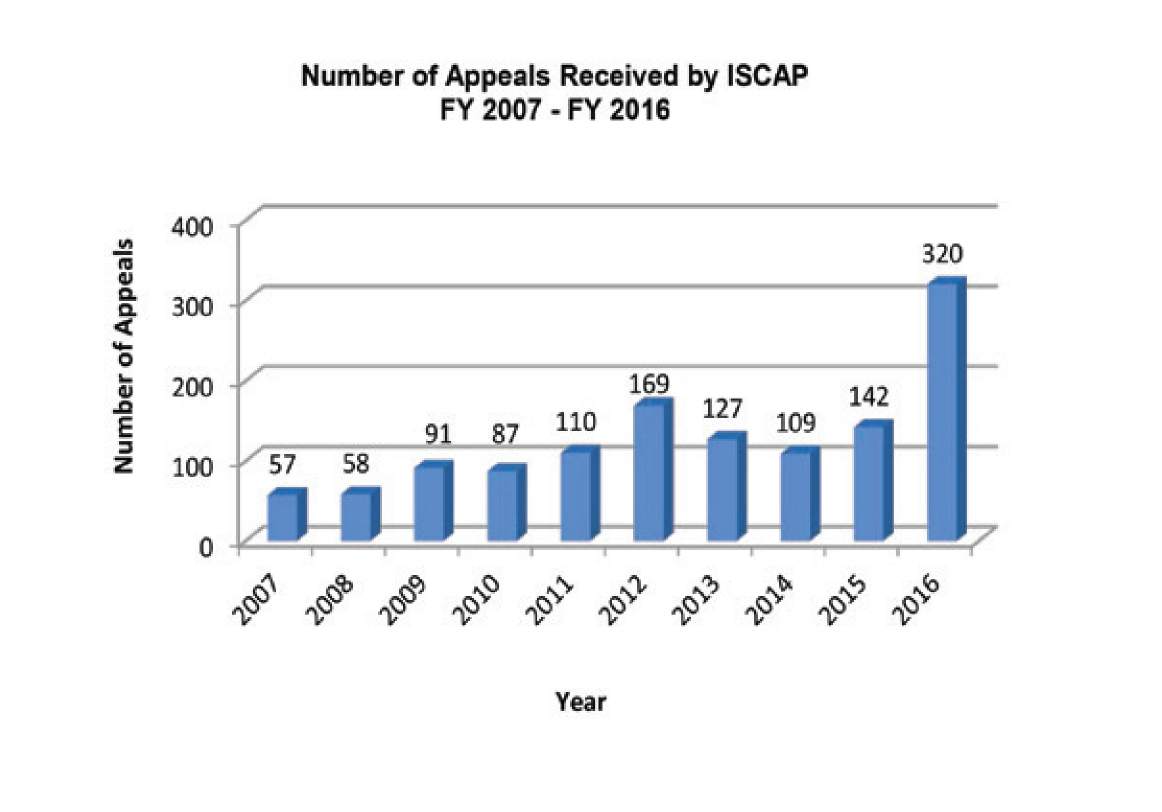
During FY 2016, the ISCAP continued to allocate most of its time and resources to processing MDR appeals. Appellants properly filed MDR appeals with the ISCAP in accordance with E.O. 13526 and the ISCAP's bylaws, 32 CFR part 2003. The ISCAP decided upon 31 MDR appeals, containing a total of 190 documents, including six motion picture recordings. The documents within these MDR appeals were classified either in part or in their entirety. The ISCAP affirmed the prior agency declassification decisions in 102 documents (54 percent). This comparatively high percentage of affirmed documents in FY 2016 is due to a single appeal in which 77 documents, consisting of detailed summaries of hundreds of Central Intelligence Agency reports issued monthly over a period of several years, were determined to require continued classification in full. The ISCAP declassified 30 documents (16 percent) in their entirety, and declassified 58 documents (30 percent) in part. Although the number of appeals and the number of documents decided upon by the ISCAP in FY 2016 are reduced when compared with previous years, the total page count for documents reviewed is a new record—5,150 pages—surpassing the previous record by over 900 pages. The reduced appeal and document count and increased page count for FY 2016 can be explained largely due to the completion of a single appeal, 2002-0049, which consisted of 16 documents totaling over 2,500 pages. That appeal was for the Central Intelligence Agency's 1969 multivolume history of the U-2 and A-12 Oxcart reconnaissance aircraft programs.

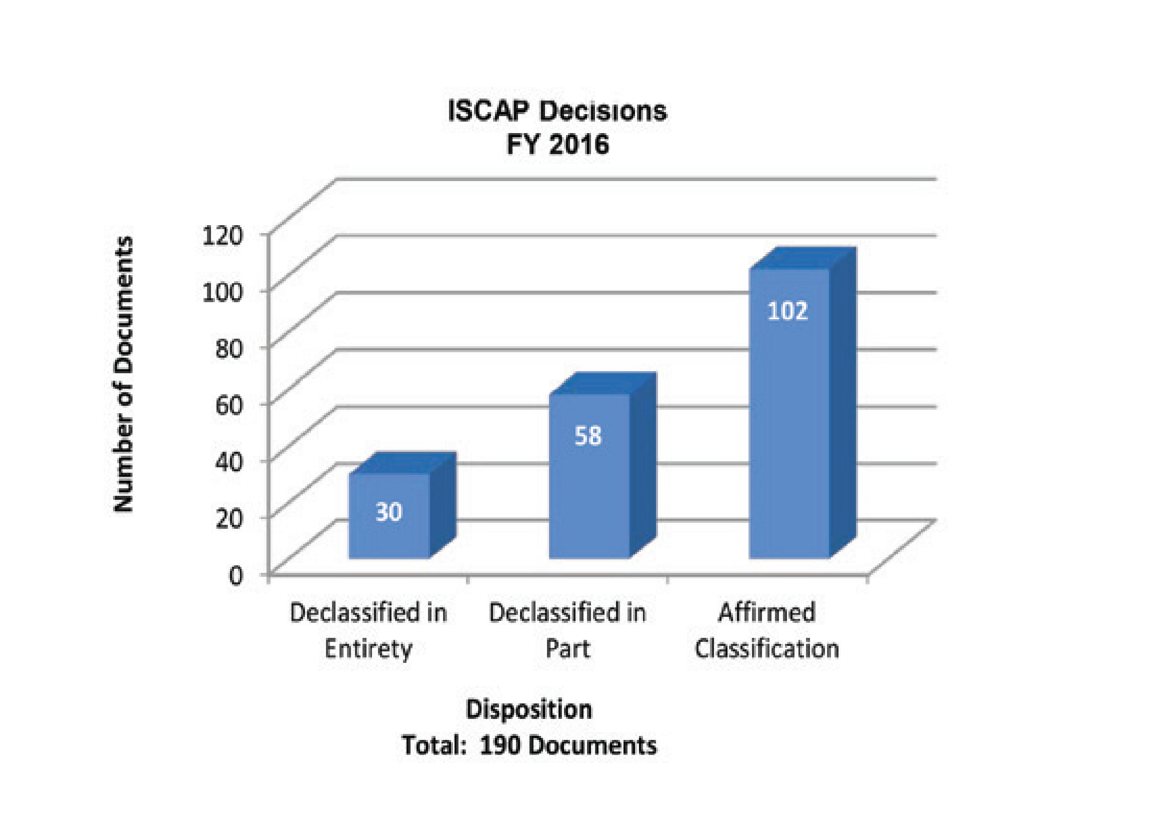
Since May 1996, the ISCAP has decided upon a total of 2,597 documents. Of these, the ISCAP declassified additional information in 73 percent of the documents. Specifically, the ISCAP declassified 724 documents (28 percent) in their entirety, declassified 1,166 documents (45 percent) in part, and fully affirmed the original decisions of agencies in 707 documents (27 percent).

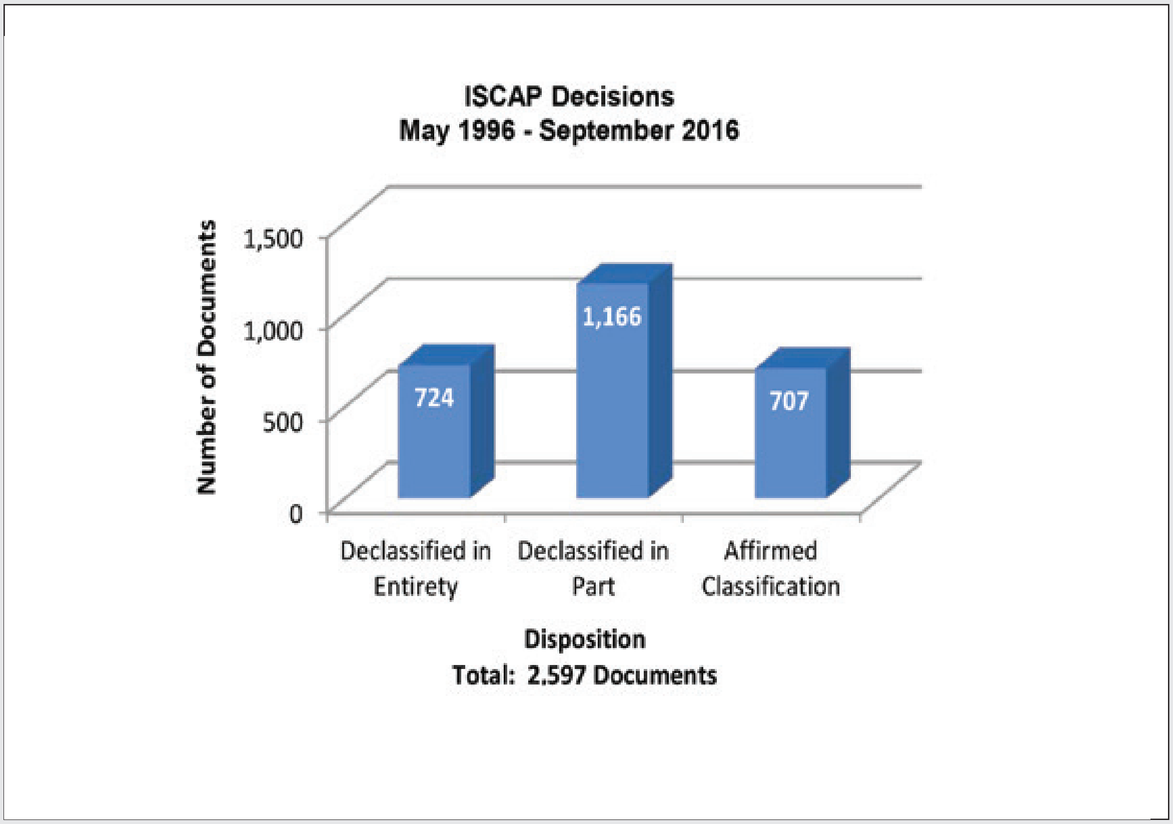
Observers of the work of the ISCAP over the past several years will note that the number of appeals received by the ISCAP in FY 2016—320 appeals—is a new record by a large margin. The dramatic increase in appeals received in FY 2016 is due in large part to the direct appeal to the ISCAP of MDR requests for which an agency failed to provide a final response within one year. In FY 2016, 71 percent of new appeals were in this category, compared with 18 percent in FY 2014 and 24 percent in FY 2015. Appellants who file multiple appeals to the ISCAP because of the expiration of the one-year timeline as allowed by the ISCAP bylaws should understand that the agency to which the request was originally filed is required by ISOO Notice 2013-03 to continue to process those appeals and to provide updates to the appellant and to the ISCAP staff when additional information is released for those requests. The ISCAP understands that appellants will continue to appeal MDR requests to the ISCAP because of the expiration of the timelines specified in the ISCAP bylaws. Appellants, however, should not expect the ISCAP to adjudicate those appeals quickly, which remain the responsibility of the receiving agency to process.

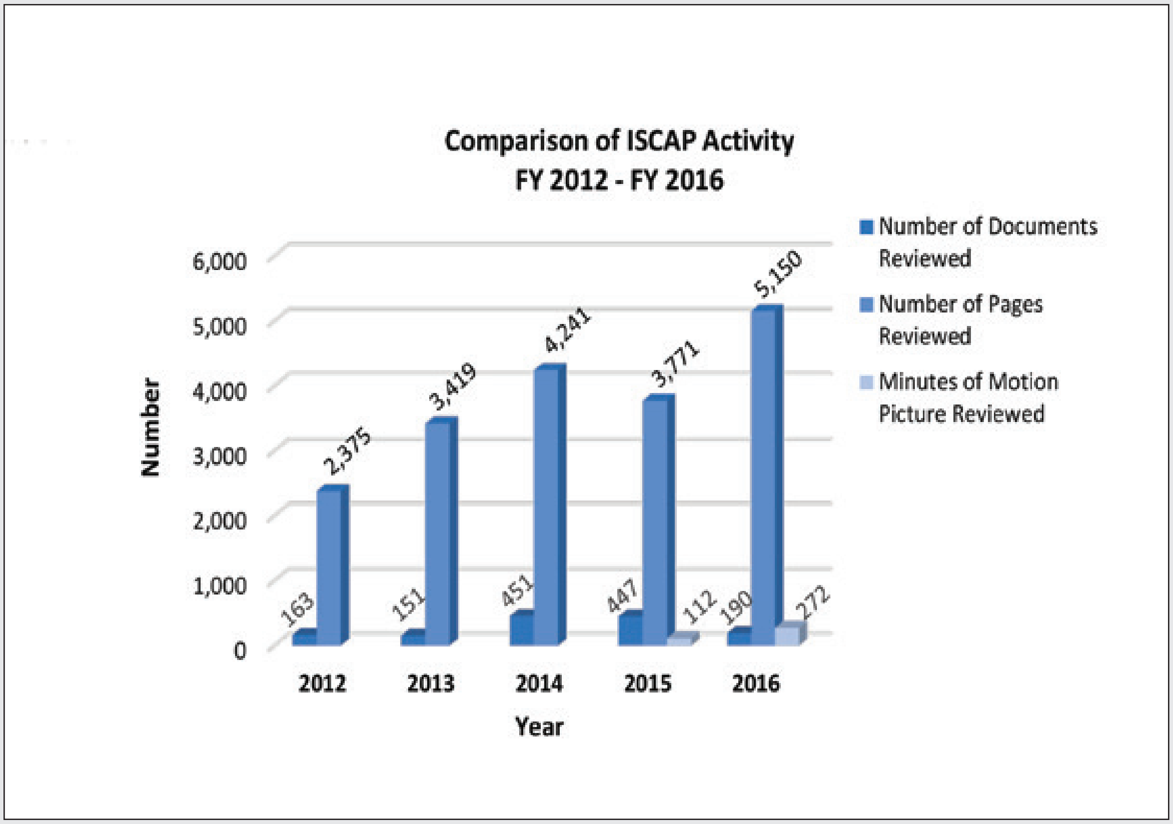
As the highest appellate authority for classification and declassification decisions, the ISCAP has a responsibility to make the most efficient use of its time. The designated liaisons of the constituent agencies and the ISCAP staff meet twice a month for several hours at a time to discuss appeals, and the ISCAP takes as much time as it deems necessary to make as complete and informed a decision as it can for each appeal. Because of the limited capacity of the ISCAP to decide on MDR appeals, the selection and prioritization of appeals are critical parts of the process. The ISCAP has provided information on its website that explains the several factors considered in the selection and prioritization of appeals. The ISCAP remains committed to resolving old appeals, but other factors—including the type of appellant, whether the appeal will result in a decision on information not previously decided upon by the ISCAP, and the size and complexity of the appeal—are taken into account.

Moose Falls, Yellowstone National Park.
Photo courtesy of National Park Service


Number of Appeals Received by ISCAP
FY 2007 - FY 2016
Number of Appeals
400
300
200
100
0
57
58
91
87
110
169
127
109
142
320
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
Year


ISCAP Decisions
FY 2016
Number of Documents
120
100
80
60
40
20
0
30
58
102
Declassified in Entirety
Declassified in Part
Affirmed Classification
Disposition
Total: 190 Documents


ISCAP Decisions
May 1996 - September 2016
Number of Documents
1,500
1,000
500
0
724
1,166
707
Declassified in Entirety
Declassified in Part
Affirmed Classification
Disposition
Total: 2,597 Documents


Comparison of ISCAP Activity
FY 2012 - FY 2016
Number of Documents Reviewed
Number of Pages Reviewed
Minutes of Motion Picture Reviewed
Number
6,000
5,000
4,000
3,000
2,000
1,000
0
163
2,375
151
3,419
451
4,241
447
3,771
112
190
5,150
272
2012
2013
2014
2015
2016
Year

Classification Challenge Appeals

During FY 2016, the ISCAP did not adjudicate any classification challenge appeals filed by an authorized holder of classified information, as provided for in section 1.8 of the Order.

Exemptions from Declassification

One important function of the ISCAP is to approve agency requests for exemptions to automatic declassification at 25, 50, and 75 years. This is usually done in the form of declassification guides, which must be updated as circumstances require, but at least once every five years. Each agency whose existing declassification guide was approved in 2012 must have submitted a revised declassification guide to the ISCAP by December 31, 2016. The ISCAP will devote a considerable proportion of its time to the review and approval of declassification guides in 2017. At the conclusion of this process, ISOO will publish as an ISOO Notice an updated list of agencies with approved exemptions 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 ISCAP recently declassified for public use. Section 5.3(b)(4) of the Order requires that the ISCAP "appropriately inform senior agency officials and the public of final ISCAP decisions on appeals under sections 1.8 and 3.5 of this order." This requirement is important for two reasons. First, the ISCAP 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 ISCAP to provide senior agency officials (and agency declassification staffs) and the public with its decisions and fulfill this requirement.

ISCAP Appeals Status Log

The ISCAP staff posts on its website a status log, updated quarterly, which 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.

Zion National Park, Utah. *Photo courtesy of Bob Skwirot*

Crater Lake National Park, Oregon. *Photo courtesy of Bob Skwirot*

ISCAP Members*

John P. Fitzpatrick, Chair
National Security Council

Garry P. Reid
Department of Defense

Mark A. Bradley
Department of Justice

Nicholas M. Murphy
Department of State

Sheryl J. Shenberger
National Archives and Records Administration

Jennifer L. Hudson
Office of the Director of National Intelligence

Executive Secretary*

William A. Cira, Acting Director
Information Security Oversight Office

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.**

**Note: The individuals named in these sections were in these positions as of the end of FY 2016.*

Note: Section 5.3(a)(2) of E.O. 13526 provides for the appointment of a temporary representative to the ISCAP 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.*

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 2016 is $16.89 billion. This includes the cost estimates of the Intelligence Community (IC)*, which total $2.38 billion. The IC costs comprise 14.10 percent of the total Government costs.

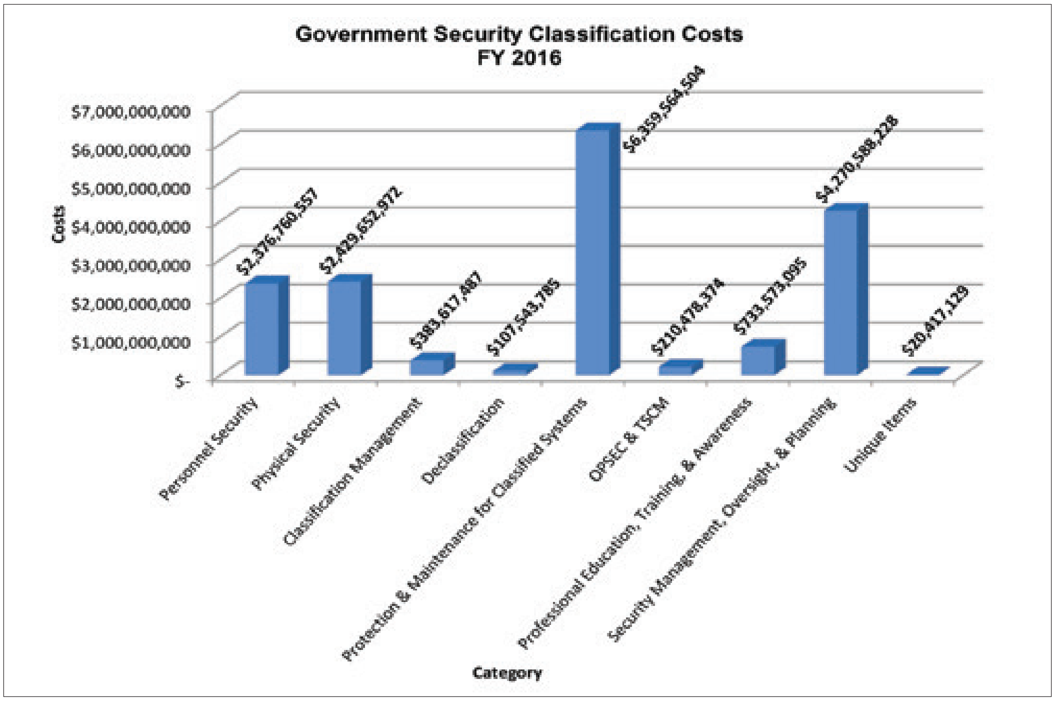
For FY 2016, agencies reported $2.38 billion in estimated costs associated with Personnel Security, an increase of $426.81 million, or 22 percent. The majority of this increase is attributed to an increased number of background investigations.

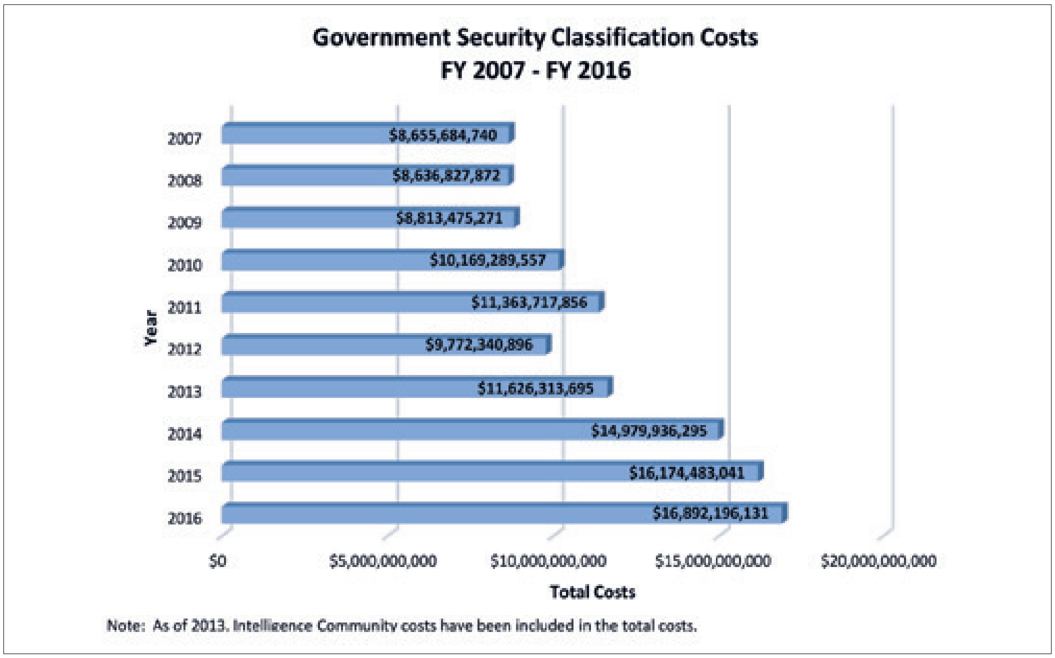
Estimated costs associated with Physical Security were $2.43 billion, an increase of $113.67 million, or 4.91 percent. Increased costs were due primarily to the purchase and installation of security equipment, such as alarms, cameras, intrusion detection systems and access control systems.

Estimated costs associated with Classification Management were $383.62 million, an increase of $16.18 million or 4 percent. This cost remains relatively steady compared to last year.

Estimated costs associated with Declassification were $108.54 million, an increase of $2.04 million, or 2 percent.

**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*





Note: As of 2013, Intelligence Community costs have been included in the total costs.

Estimated costs associated with Protection and Maintenance for Classified Information Systems were $6.36 billion, a decrease of $1.68 billion, or 21 percent. This cost fluctuates every year, primarily determined by the purchase or upgrade of systems.

Estimated costs associated with OPSEC and TSCM were $210.48 million, a decrease of $15.62 million, or 7 percent.

The estimated costs for Professional Education, Training, and Awareness were $733.57 million, an increase of $46.90 million, or 7 percent.

Estimated costs associated with Security Management, Oversight, and Planning were $4.27 billion, an increase of $1.80 billion, or 73 percent. This increase is partly attributed to a single agency better understanding the costs that are counted in this category, and partly to another agency developing and updating computer-based training modules for national security information.

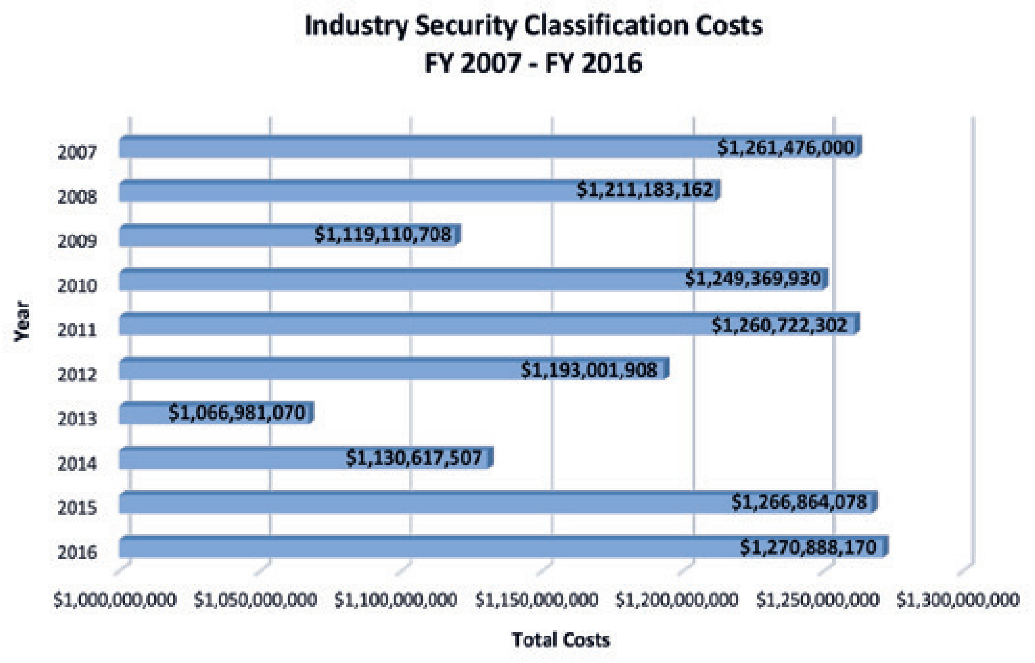
Estimated costs associated with Unique Items were $20.42 million, an increase of $5.67 million, or 38 percent. Costs included maintenance costs for sensitive compartmented information facilities (SCIF), leased classifier copiers, microfilm development, and installation and connectivity charges for access to SCIFs and Continuity/Emergency Operations Centers.

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 2016, the Defense Security Service collected industry cost data and provided the estimate to ISOO.

Cost estimate data is 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 2016 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 2016 within industry was $1.27 billion; an increase of $4.02 million, or .32 percent.



National Industrial Security Program

ISOO is responsible for implementing and overseeing the National Industrial Security Program (NISP) established 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 2016. The major issues discussed during these meetings included the timeliness of processing contractor personnel security clearances, the assessment and authorization process for contractor information systems to process classified information, industry implementation of national insider threat policies, and the revisions of the NISPOM and 32 CFR part 2004, NISP Directive No.1, to incorporate required changes.

The NISPPAC convenes several working groups comprised of both government and industry participants to address NISPPAC action items and issues of mutual interest and concern. These permanent and ad hoc working groups enhance the NISPPAC by facilitating collaboration, 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 continued 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 newly established National Background Investigations Bureau within the Office of Personnel Management, 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 the impact of the inability to share eligibility and access information across the various agency systems, the impact of the personnel security investigations backlog on industry contract performance, and the lengthy timelines of reinvestigations that impact industry's ability to access government bases and installations.

The Information Systems Authorization 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 assessment and authorization process, to include industry's implementation of the risk management process for system assessments and authorizations during FY 2016.

As a result of the issuance of a NISPOM change in FY 2016 that requires contractors to establish insider threat programs as part of the NISP, a NISPPAC Insider Threat working group was established. The working group facilitates information sharing among the cognizant security agencies (CSA) regarding their oversight processes and provides industry the opportunity to share their experiences in implementing insider threat programs.

The Department of Defense, in its role as the NISP Executive Agent, is working with ISOO, the other CSAs, and industry on a comprehensive update to the NISPOM that is expected to be issued in FY 2018. At the same time, ISOO is working on a revision to the current 32 CFR part 2004 to make it much more comprehensive. The directive has not been updated since 2010. The rewrite is an opportunity to establish insider threat responsibilities for the executive branch agencies that issue contracts requiring access to classified information, including DHS as a CSA as a result of the issuance of Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," in 2015, and establishing consistent standards for all CSAs for determining contractor eligibility for access to classified information, and for providing oversight. The revision was issued by the Office of Management and Budget in January 2017 as a proposed rule and request for public comments.

ISOO continued to lead an inter-agency effort directed at the sharing and safeguarding of classified information with certain private or other non-federal entities. This work ultimately resulted in an amendment to E.O. 12829 that established DHS as the fifth CSA responsible for overseeing the Classified Critical Infrastructure Protection Program (CCIPP). In order to implement the CCIPP, ISOO led the effort in formulating additional NISP procedures for sharing and safeguarding classified information with certain private or other non-federal entities. These national level procedures were approved by the President in December 2016, and are likely to serve as a catalyst for increased classified information sharing with private and other non-federal entities.

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 2016, 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.**

Controlled Unclassified Information

Background

Existing laws, regulations, and Government-wide policies identify unclassified information types such as privacy, security, proprietary interests, and law enforcement investigations that require specific distribution or safeguarding. However, authorities are frequently silent on how to achieve these protections. The result was a proliferation of more than 100 different policies and practices for the creation and handling of such information across the executive branch. This ad hoc approach resulted in mishandled information, impeded appropriate information sharing, and created confusion regarding safeguarding and dissemination practices, especially when sharing information with non-federal partners. Such problems were further aggravated by agency policies that were sometimes unavailable to public view.

The CUI program was established to reform the inconsistent and sometimes conflicting patchwork of agency-specific policies, procedures, safeguarding measures and labels, used to handle sensitive unclassified information throughout the executive branch. The National Archives and Records Administration (NARA) is the CUI Executive Agent (EA). The Archivist of the United States delegated EA responsibilities to the Director of ISOO.

This information security and management reform established the concept of standardized CUI categories and subcategories as the exclusive means for agencies to designate unclassified information that requires safeguarding and dissemination controls. The CUI program also requires that designation of information as CUI must be consistent with a law, regulation, or Government-wide policy that requires or permits the protection of such information.

At the request of the CUI EA, Federal agencies reviewed their respective sensitive but unclassified information practices and submitted to ISOO those categories and subcategories, with supporting citations in law, regulation, and/or Government-wide policy that the agency intends to continue to employ. ISOO reviewed more than 2,200 proposed category and subcategory submissions, and worked with Federal agencies to consolidate redundancies and provide consistency among like categories to build the baseline CUI Registry. The CUI Registry defines the scope of all information covered under the CUI Program and provides a single source for descriptions of unclassified information that requires protection, across the executive branch.

The CUI EA worked with an extensive list of stakeholders, including the White House; Federal agencies; State, local, Tribal, private sector, and educational entities; public-interest groups; and the general public, to develop a regulation that provides consistent direction for designating, marking, safeguarding, disseminating, decontrolling, and disposing of CUI for all agencies and their stakeholders. ISOO will continue to develop and issue directives as necessary to implement and maintain the CUI program.

Concurrent with development of a CUI Federal regulation, ISOO also undertook steps to address information systems requirements for non-Federal organizations by jointly developing with the National Institute of Standards and Technology (NIST) the NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," June 2015.[1] NIST SP 800-171 describes information systems security requirements for CUI based on the conditions of

[1] NIST SP 800-171, Revision 1, was published in December 2016 under the updated title "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

Haleakala National Park, Maui, Hawaii. *Photo courtesy of Bob Skwirot*

the non-Federal environment. The publication promotes consistent implementation of defined and rigorous electronic safeguards for the protection of CUI and the compliance of non-Federal organizations, with statutory and regulatory requirements.

Policy

ISOO developed "Controlled Unclassified Information," 32 CFR part 2002, after consulting with affected agencies through the CUI Advisory Council and other CUI stakeholders. Stakeholders were provided multiple opportunities to provide input regarding existing procedures for handling information that laws, regulations, and Government-wide policies require agencies to control. Based on this iterative strategy, ISOO submitted a proposed Federal rule to the Office of Management and Budget (OMB) in May 2015, to establish a consistent baseline policy throughout the executive branch.

Following the proposed rule's publication, the regulation underwent an additional four rounds of executive branch-wide interagency comment, one round of public comment, a NARA leadership review, discussions with individual agencies, and a round of White House comment (including OMB, the Executive Office of the President and the National Security Council). ISOO and NARA's Strategy and Performance Division adjudicated approximately 1,000 comments and proposals during FY 2016, following an initial round of approximately 800 adjudications reported in FY 2015. The nearly 1,800 total comments and proposals were balanced, individually and collectively, across the more than 150 agencies, departments, bureaus and other components within the executive branch. Following rigorous and deliberate evaluation, 32 CFR part 2002 was published in the Federal Register on September 14, 2016.

32 CFR part 2002 establishes policy for designating, safeguarding, disseminating, marking, decontrolling, and destroying CUI; guidelines for self-inspection; and oversight requirements for agency CUI programs. The regulation impacts Federal executive branch agencies that handle, possess, use, share or receive CUI and their non-Federal stakeholders that operate, use, or have access to Federal information and information systems on behalf of an agency. Significant features of the regulation include: (1) drawing attention to any specified protections required on certain information by law, regulation, or Government-wide policy, (2) determining the overall marking structure for CUI while providing some latitude for agencies, and (3) setting electronic safeguarding standards for CUI.

Oversight and Liaison

CUI oversight and liaison efforts are designed to assist executive branch agencies and departments in developing, implementing, and sustaining their respective CUI programs, and to offer assistance and guidance to non-Federal entities who, through agreements, must also implement the CUI program.

In FY 2016, ISOO continued its efforts to assist agencies in preparing for the implementation of the CUI program by:

- Conducting formal appraisals of existing agency practices;
- Consulting with executive branch agencies and supporting elements (i.e., component agencies and non-Federal entities) on strategies and practices related to implementation; and
- Presenting briefings, training/awareness sessions, and panel discussions, to raise awareness of key program elements, implementation timelines, and features of an organizational program that will meet Federal CUI requirements.

ISOO is developing a formal inspection program to monitor agency efforts related to implementation and will provide agencies with recommendations and required actions in order to fully comply with the requirements of 32 CFR part 2002, and the CUI Registry. ISOO will conduct on-site inspections of agencies that comprise the 28-member CUI Advisory Council on a 4-year, recurring schedule. Agencies that are not part of the CUI Advisory Council will receive on-site inspections based on their annual report submissions, upon their request, or the Director of ISOO's discretion.

In FY 2016, ISOO began the development of standardized inspection criteria for evaluating agency programs. Throughout FY 2017, ISOO will continue to refine the inspection criteria with the CUI Advisory Council.

Implementation by the Executive Branch

On September 14, 2016, ISOO issued target dates for phased implementation of the CUI Program in CUI Notice 2016-01, "Implementation Guidance for the Controlled Unclassified Information Program."

By May 13, 2017 (180 days of the effective date of 32 CFR part 2002):

- All agencies must publish an implementing policy for the CUI Program and rescind all existing policies that are not consistent with 32 CFR part 2002.

- All agencies must assess the current configuration of information systems and plan for the transition to the standard established in the regulation. By November 14, 2017 (one year of the effective date of the 32 CFR part 2002), agencies must develop a strategy or plan to modify all systems that contain or process CUI.

Within 180 days of the effective date of the agency CUI implementing policy:

- All agencies must develop and deploy CUI training to all agency employees that work with CUI. All agency employees must receive CUI training within 180 days of the release of the agency's CUI training course(s).
- All agencies must implement and/or verify that all physical safeguarding requirements, as described in 32 CFR part 2002 and agency policy, are in place.
- If applicable, all subordinate components must publish implementing policies.

On November 1, 2017, all agencies must submit their first annual report to ISOO, evaluating and assessing agency actions and activities related to implementing and sustaining the CUI Program.

CUI Registry and Website

As the repository for common definitions, protocols, and procedures for properly marking, safeguarding, disseminating, and decontrolling unclassified information, the CUI Registry is a central element of the CUI Program. As of September 30, 2016, the online CUI Registry includes descriptions for 23 categories and 85 subcategories of unclassified information, supported by 330 unique control citations and 98 unique sanction citations in the United States Code (USC), Code of Federal Regulations (CFR), and Government-wide policies.

ISOO continues to update the CUI Registry based on identification of unclassified information that requires protection based on law, regulation, and/or Government-wide policies. Changes to categories and subcategories are made after consulting with the CUI Advisory Council. Control and sanction authority references are updated annually based on updates to the USC and CFR, and review of Government-wide policy documents.

Additions to the CUI Registry during FY 2016 included 32 CFR part 2002; CUI Notice 2016-01, "Implementation Guidance for the Controlled Unclassified Information Program;" and the CUI Marking Handbook. Also during FY 2016, all control and sanction citations were reviewed and reconfirmed for applicability to the CUI Program.

In addition to the online Registry, the CUI web presence provides updates, handouts, training modules, reports, and general information. Providing clear and readily accessible direction promotes more consistent protection and sharing of sensitive information both internally and externally.

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

Assateague Island National Seashore, Maryland and Virginia
Photo courtesy of Bob Skwirot

Zion National Park, Utah
Photo courtesy of National Park Service

Denali National Park and Preserve, Alaska
Photo courtesy of Bob Skwirot

New River Gorge National River, West Virginia
Photo courtesy of Bob Skwirot

Redwood National Park, California
Photo courtesy of Bob Skwirot

North Cascades National Park, Washington. *Photo courtesy of National Park Service*

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100   WASHINGTON, DC 20408-0001
www.archives.gov/isoo

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE