2015 REPORT TO THE PRESIDENT

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION

Front Cover: The plantings of cherry trees originated in 1912 as a gift of friendship to the People of the United States from the People of Japan. In Japan, the flowering cherry tree, or "Sakura," is an exalted flowering plant. The beauty of the cherry blossom is a potent symbol equated with the evanescence of human life and epitomizes the transformation of Japanese culture throughout the ages (http://www.nps.gov/chbl/cherry-blossom-history.htm).

AUTHORITY

- Executive Order (E.O.) 13526, "Classified National Security Information"
- E.O. 12829, as amended, "National Industrial Security Program"
- E.O. 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities"
- E.O. 13556, "Controlled Unclassified Information"
- E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"

The Information Security Oversight Office (ISOO) is a component of the National Archives and Records Administration (NARA) and receives its policy and program guidance from the Assistant to the President for National Security Affairs.

ISOO'S MISSION

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

FUNCTIONS

- Develop implementing directives and instructions.
- Review and approve agency implementing regulations.
- Maintain liaison relationships with agency counterparts and conduct on-site and document reviews to monitor agency compliance.
- Develop and disseminate security education materials for Government and industry; monitor security education and training programs.
- Receive and take action on complaints, appeals, and suggestions.
- Collect and analyze relevant statistical data and, along with other information, report them annually to the President.

- Serve as spokesperson to Congress, the media, special interest groups, professional organizations, and the public.
- Conduct special studies on identified or potential problem areas and develop remedial approaches for program improvement.
- Recommend policy changes to the President through the Assistant to the President for National Security Affairs.
- Provide program and administrative support for the Interagency Security Classification Appeals Panel (ISCAP).
- Provide program and administrative support for the Public Interest Declassification Board.
- Review requests for original classification authority from agencies.
- Serve as Executive Agent to implement E.O. 13556 and oversee agency actions.
- Chair the National Industrial Security Program Policy Advisory Committee (NISPPAC) under E.O. 12829, as amended.
- Chair the State, Local, Tribal, and Private Sector Policy Advisory Committee under E.O. 13549.
- Serve as member of the Senior Information Sharing and Safeguarding Steering Committee under E.O. 13587.

GOALS

- Promote programs for protection of classified and controlled unclassified information.
- Reduce classification and control activity to the minimum necessary.
- Ensure that the systems for declassification and decontrol operate as required.
- Provide expert advice and guidance to constituents.
- Collect, analyze, and report valid information about the status of agency programs.

July 15, 2016

Dear Mr. President

I am pleased to submit the Information Security Oversight Office's (ISOO) Report for Fiscal Year 2015, as required by Executive Order 13526, "Classified National Security Information" (the Order).

This report provides statistics and analysis of the system of classification and declassification based on ISOO's review of Departments' and Agencies' programs. It also contains the status of agency self-assessment reporting, the National Industrial Security Program (NISP), the Controlled Unclassified Information (CUI) Program, and the cost of security classification activity.

There is good news to report. The executive branch agencies have reported a 32% decrease in their amounts of derivative classification while at the same time they reported a 30% increase over the number of pages declassified in FY 2014.

E.O. 13526 requires agencies to conduct self-inspections and report to ISOO about their self-inspection programs and findings. We are seeing that some agencies' self-inspection programs are very strong, while others still need to improve. Agency self-inspection reports include narrative self-inspection program descriptions and summaries of findings, as well as data-centric responses to specific questions about core program requirements. In nearly all of these areas agencies reported improvement in compliance from last year.

The National Industrial Security Program Policy Advisory Committee (NISPPAC) developed procedures for implementing an insider threat program, and continued to advance the government-industry partnership. ISOO contributed significant support to the administration's cyber security information sharing initiatives, guiding NISP partner agencies through the creation of novel risk management processes made effective as part of E. O. 13691 "Promoting Private Sector Cyber Security Information Sharing." 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 fulfills Executive Agent (EA) responsibilities for the CUI Program, which were designated by Executive Order 13556 to the National Archives and Records Administration. During the past year, ISOO continued to advance its policy development strategy, as its submitted proposed Federal CUI rule (the future 32 Code of Federal Regulations part 2002) underwent extensive agency and, after its publication in the Federal Register, public comment. The EA continued its CUI Program appraisal process to assist executive branch agencies in preparing for implementation by providing agency planners with a baseline for key elements of an agency CUI program. With the Office of Management and Budget and affected agencies, the EA also coordinated a timeline for phased implementation of

the CUI Program for the executive branch, which will be provided to agencies at the time of the regulation's issuance.

Upon finalization of the CUI Federal regulation, the EA will propose a single Federal Acquisition Regulation (FAR) rule that will apply the requirements of 32 CFR part 2002 and National Institute of Standards and Technology (NIST) Special Publication 800-171 *Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations*, which was developed in partnership with the NIST, to the contractor environment. This will further promote standardization to benefit non-Federal organizations that may struggle to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from various agencies for the same information creates confusion and inefficiencies.

Respectfully,

William A. Cira | Acting Director

TABLE of CONTENTS

02 CLASSIFICATION
- Original Classification Authorities
- Original Classification Activity
- Derivative Classification Activity
- Classification Challenges

09 DECLASSIFICATION
- Background
- Automatic, Systematic, and Discretionary Review
- Mandatory Declassification Review

17 REVIEWS
- Declassification Assessments
- Self-Inspections
- Classified National Security Information Program Reviews

27 INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

31 COST ESTIMATES for SECURITY CLASSIFICATION ACTIVITIES
- Background and Methodology
- Results – Government Only
- Results – Industry Only
- Results – Combined Government and Industry

35 THE NATIONAL INDUSTRIAL SECURITY PROGRAM

37 CONTROLLED UNCLASSIFIED INFORMATION
- Background
- Policy Development
- Training
- Oversight and Outreach
- CUI Registry and Website

SUMMARY of FY 2015 PROGRAM ACTIVITY

CLASSIFICATION

Executive branch agencies reported 2,199 original classification authorities (OCA), down from 2,276 reported in FY 2014.

Agencies reported 53,425 original classification decisions, an increase of 14 percent from last year.

Agencies reported using the ten-years-or-less declassification instruction for only 15 percent of original classification decisions.

Executive branch agencies reported 52,778,354 derivative classification decisions; a 32 percent decrease from FY 2014.

DECLASSIFICATION

Agencies received 8,385 initial mandatory declassification review (MDR) requests and closed 5,889 requests. The average number of days to resolve each request is 270. A total of 14,338 requests have remained unresolved for over one year. This number includes requests that have been carried over from prior years. Agencies reviewed 391,103 pages, and declassified 240,717 pages in their entirety, declassified 109,349 pages in part, and retained classification of 41,037 pages in their entirety.

Agencies received 384 MDR appeals and closed 365 appeals. The average number of days to resolve each appeal is 244. A total of 396 appeals have remained unresolved for over one year.

Agencies reviewed 14,308 pages on appeal, and declassified 4,597 pages in their entirety, declassified 6,057 pages in part, and retained classification of 3,654 pages in their entirety.

Under automatic declassification, agencies reviewed 84,424,836 pages and declassified 36,042,022 pages of historically valuable records.

Under systematic declassification reviews, agencies reviewed 2,625,373 pages, and declassified 706,859 pages.

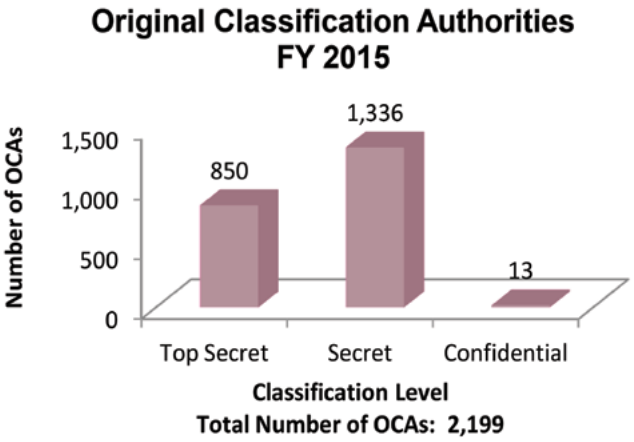
Under discretionary declassification reviews, agencies reviewed 142,649 pages, and declassified 30,708 pages.

Under automatic, systematic, and discretionary declassification reviews, a total of 87,192,858 pages were reviewed for declassification and 36,779,589 pages were declassified.

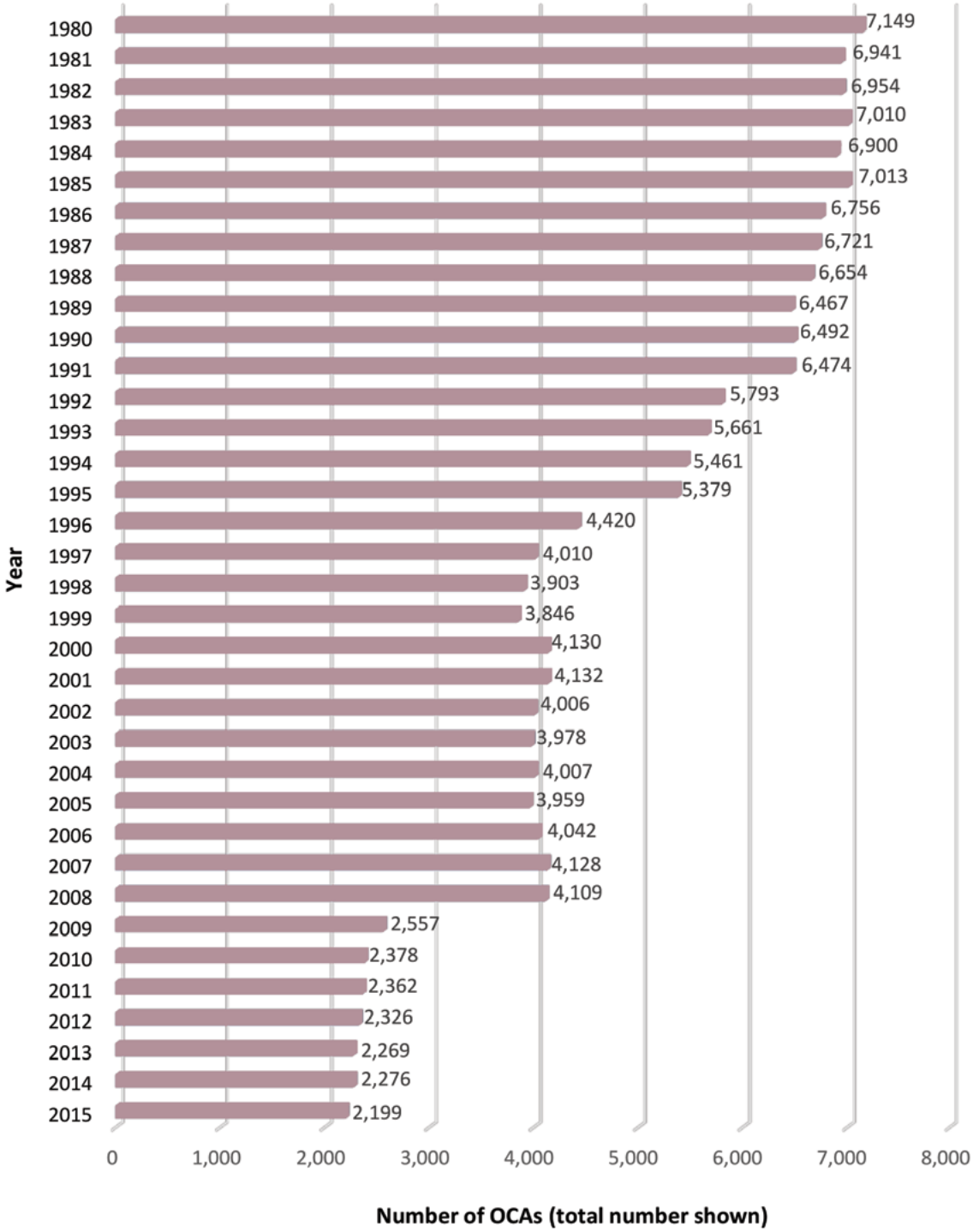
CLASSIFICATION

Original Classification Authorities

Original classification authorities, also called original classifiers, are those individuals designated in writing, either by the President, by selected agency heads, or by designated senior agency officials with Top Secret original classification authority, to classify information in the first instance. Only original classifiers are authorized to determine what information, if disclosed without authorization, could reasonably be expected to cause damage to national security. Original classifiers must be able to identify or describe the damage. Agencies reported 2,199 OCAs in FY 2015; a 3.38 percent decrease from the 2,276 reported in FY 2014.



Original Classification Authorities
FY 1980–FY 2015



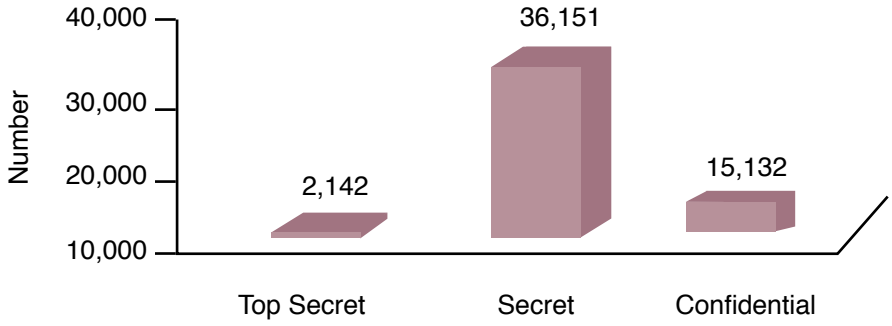
Original Classification Activity

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 cause damage to the national security.

The process of original classification must always include a determination by an OCA of the concise reason for the classification that falls within one or more of the authorized categories of classification, the placement of markings to identify the information as classified, and the date or event when the information will become declassified unless it is appropriately referred, exempted, or excluded from automatic declassification. By definition, original classification precedes all other aspects of the security classification system, including derivative classification, safeguarding, and declassification.

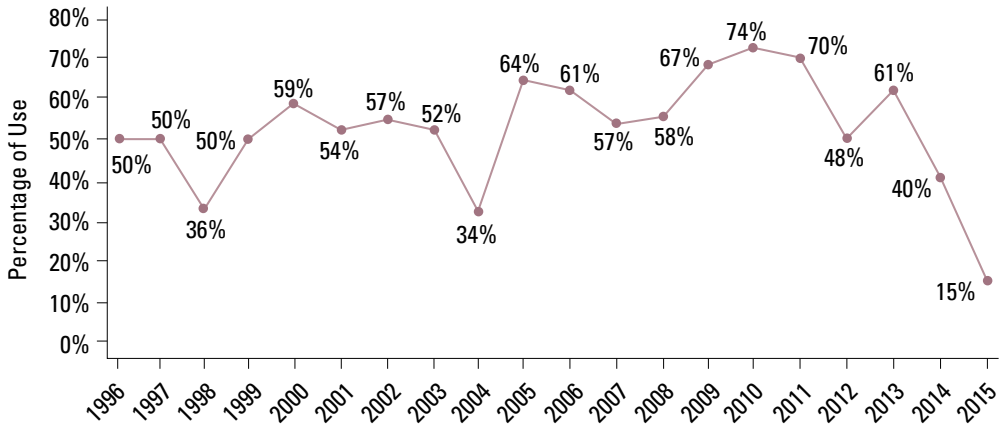
The agencies reported 53, 425 original classification decisions for FY 2015, using the ten-years-or-less declassification instruction only 15 percent of the time.

Original Classification Activity, FY 2015

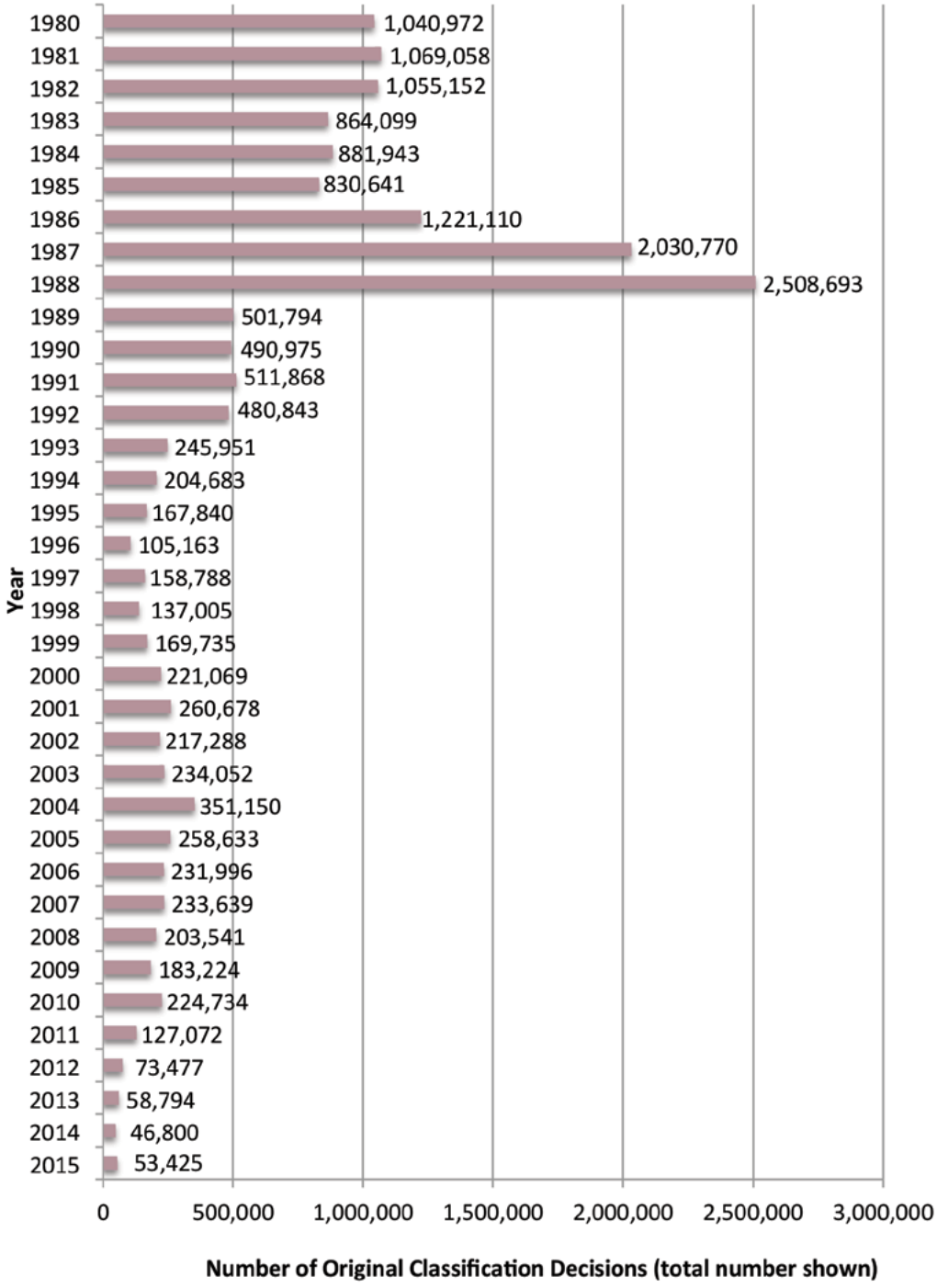


Total Number of Original Classification Decisions: 53,425

Use of the "Ten Years or Less" Declassification Instruction
FY 1996 – FY 2015



Original Classification Activity
FY 1980–FY 2015



Derivative Classification Activity

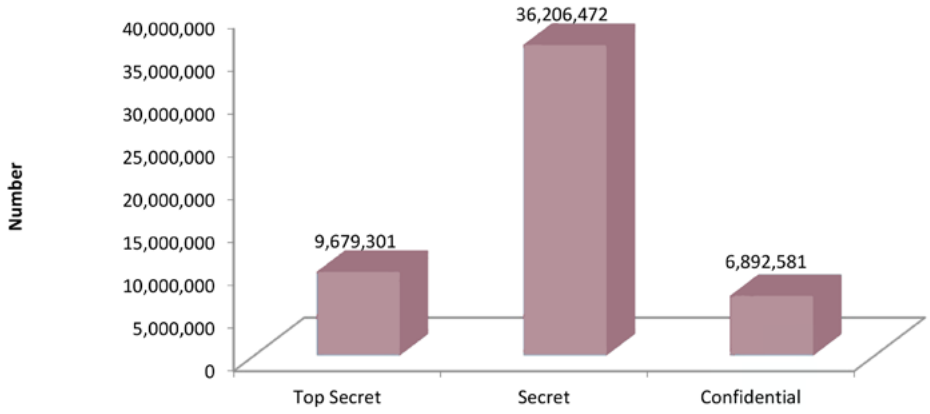
Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified. Information may be derivatively classified in two ways: (1) through the use of a source document, usually correspondence or a publication generated by an OCA; or (2) through the use of a classification guide. A classification guide is a set of instructions issued by an OCA that identifies elements of information regarding a specific subject that must be classified, and establishes the level and duration of classification for each such element. Classification guides provide consistency and accuracy to classification decisions.

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

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

Agencies reported an estimated total of 52.78 million derivative classification decisions in FY 2015, a decrease of 32 percent from FY 2014. This drop in derivative classification activity can be attributed to a number of agencies that reported a decrease in their numbers.

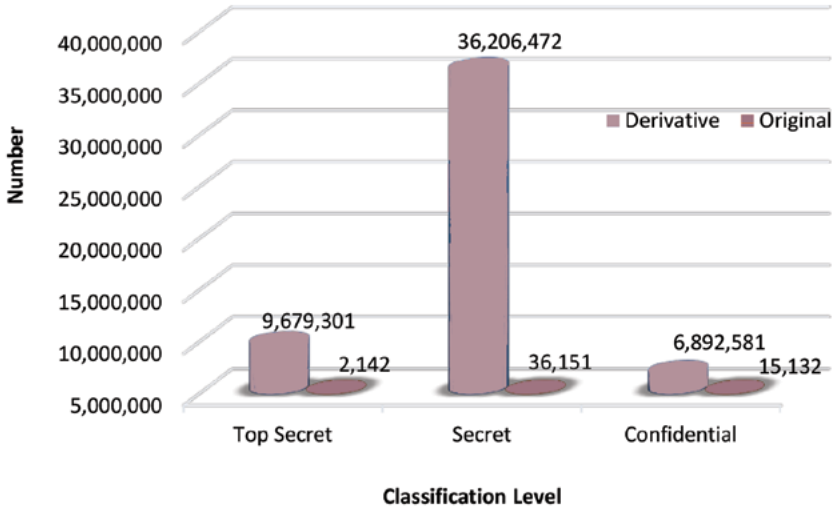
Derivative Classification Activity, FY 2015



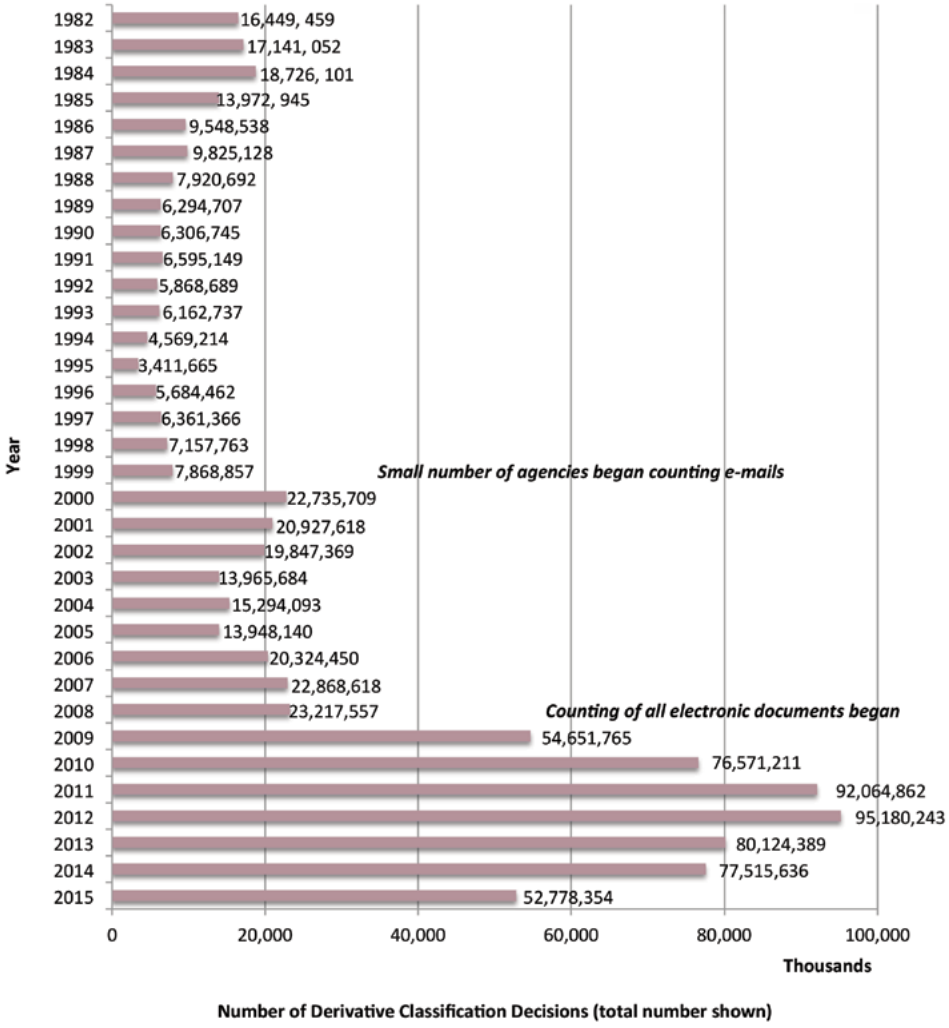
Classification Level

Total Number of Derivative Classification Decisions: 52,778,354

Derivative Classification Decisions vs Original Classification Decisions
FY 2015



Derivative Classification Activity, FY 1982 – FY 2015



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 952 formal challenges in FY 2015; 403 (42.33 percent) were fully affirmed at their current classification status with 411 (43.17 percent) being overturned either in whole or in part, and 138 (14.50 percent) challenges remaining open.

DECLASSIFICATION

Background

Declassification is defined as the authorized change in status of information from classified to unclassified and is an integral part of the security classification system. There are four declassification programs within the executive branch: automatic declassification, systematic declassification review, discretionary declassification review, and mandatory declassification review.

Automatic declassification removes the classification of information at the close of every calendar year when that information reaches the 25-year threshold.

Systematic declassification review is required for those records exempted from automatic declassification.

Discretionary declassification review is conducted when the public interest in disclosure outweighs the need for continued classification, or when an agency determines the information no longer requires protection and can be declassified earlier.

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

Since 1996, statistics reported for systematic declassification review and automatic declassification were combined because the execution of both programs is usually indistinguishable. In FY 2010, however, agencies began to report automatic, systematic, discretionary and mandatory declassification numbers separately. Together, these four programs are essential to the viability of the classification system and vital to an open government.

Automatic, Systematic, and Discretionary Declassification Review

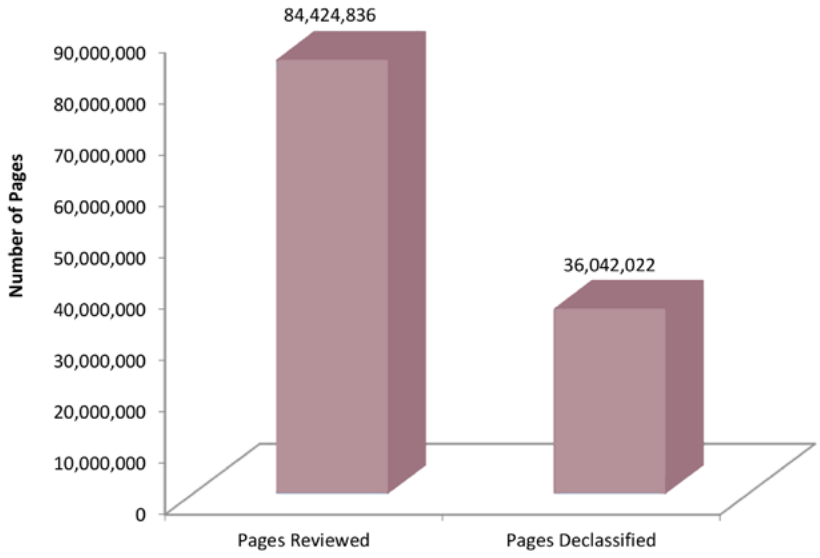
During FY 2015, a total of 87.19 million pages were reviewed under the automatic, systematic, and discretionary declassification programs and 39.78 million pages (42 percent) were declassified*. This is a 26 percent increase in the number of pages reviewed and a 30 percent increase in the number of pages declassified during FY 2014.

Under automatic declassification review, agencies reviewed 84.42 million pages and declassified 36.04 million pages (43 percent). Under systematic declassification review, agencies reviewed 2.63 million pages and declassified 706,859 pages (27 percent). Under discretionary declassification review, agencies reviewed 142,649 pages and declassified 30,708 pages (22 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*

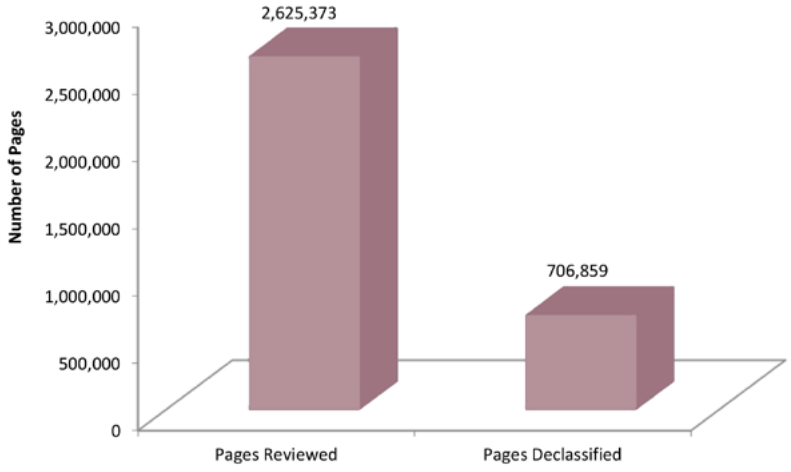
FY 2015

Number of Pages Reviewed and Declassified
for Automatic Declassification



FY 2015

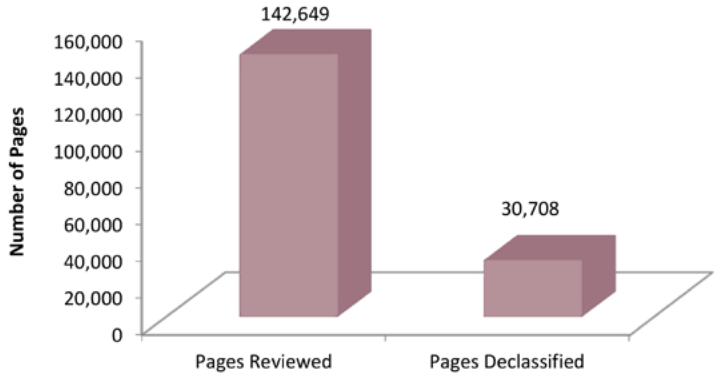
Number of Pages Reviewed and Declassified
for Systematic Declassification



FY 2015

Number of Pages Reviewed and Declassified

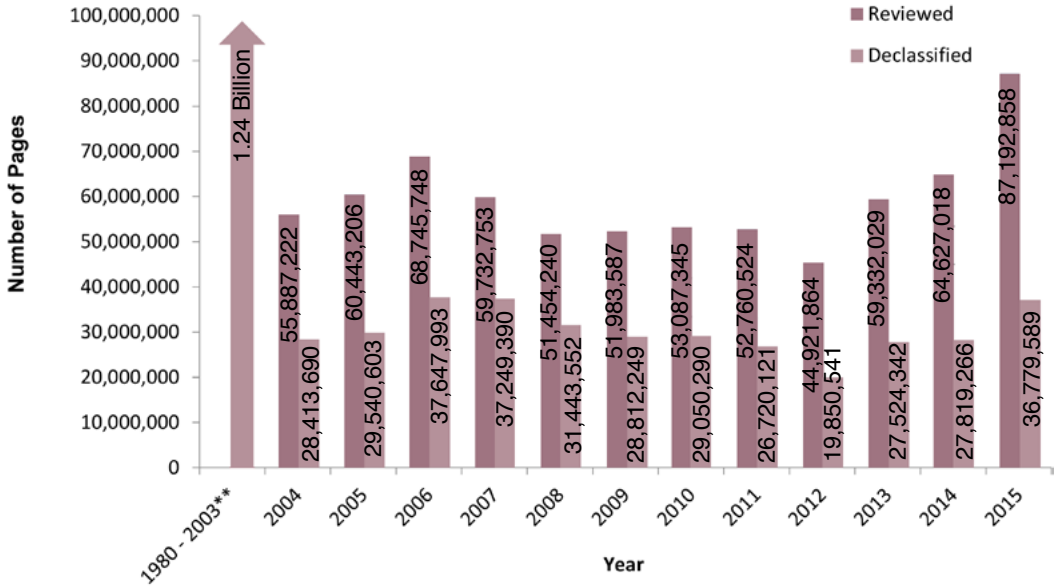
for Discretionary Declassification



Total Number of Pages Reviewed and Declassified*

Automatic, Systematic, and Discretionary Declassification Review

FY 1980 – FY 2015



* Excludes Mandatory Declassification Review

** Number of pages reviewed not available

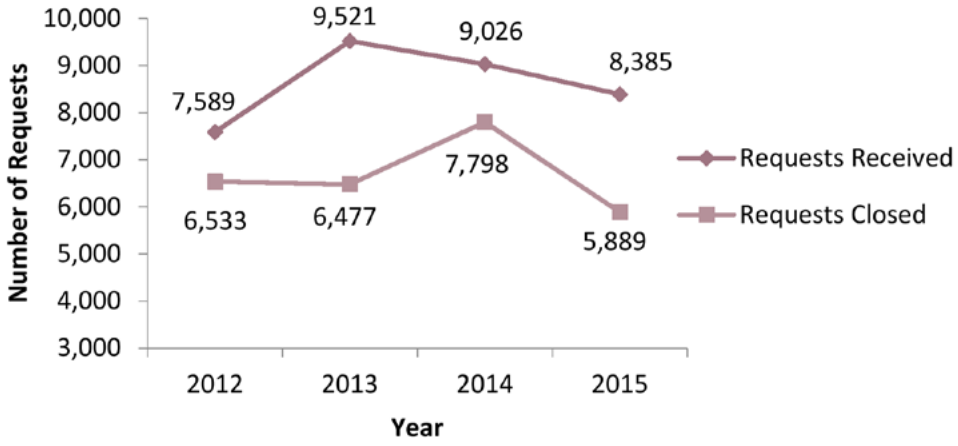
Mandatory Declassification Review

The mandatory declassification review (MDR) process requires a review of specific classified national security information in response to a request seeking its declassification. The public must make MDR requests in writing and each request must contain sufficient specificity describing the record to allow an agency to locate the record with a reasonable amount of effort. MDR remains popular with some researchers as a less litigious alternative to requests under the Freedom of Information Act (FOIA), as amended. It is also used to seek the declassification of Presidential papers or records not subject to FOIA.

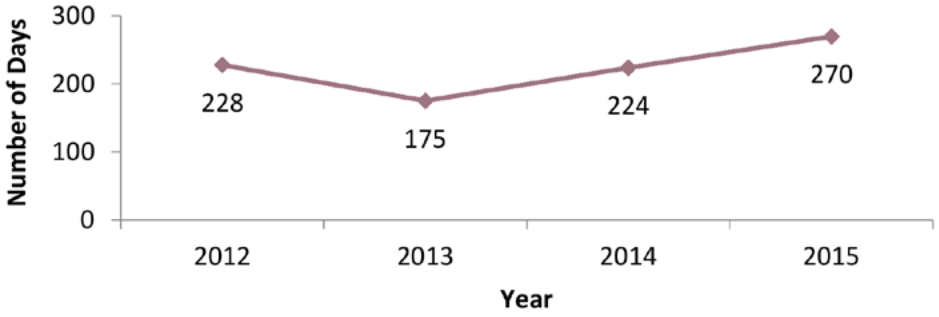
The FY 2015 data specify the number of requests and appeals received, the number that remain unresolved for over one year, and the average number of days it takes to resolve each request and appeal. The report also displays the number of referred MDR requests and appeals to more accurately reflect the MDR workload of agencies. The number of referred MDR requests and appeals are not included in the statistical calculations to prevent duplicate counts.

MDR Requests

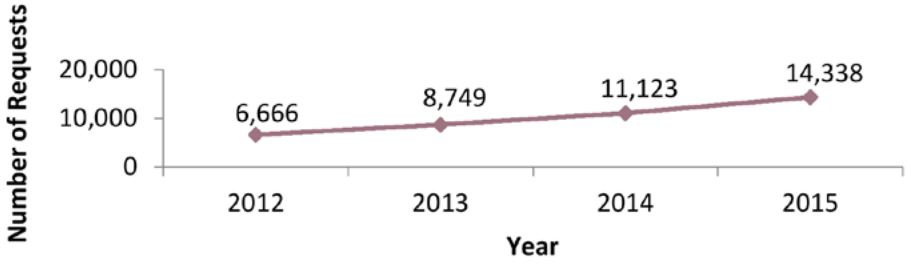
Mandatory Declassification Review Requests Received and Closed
FY 2012 – FY 2015



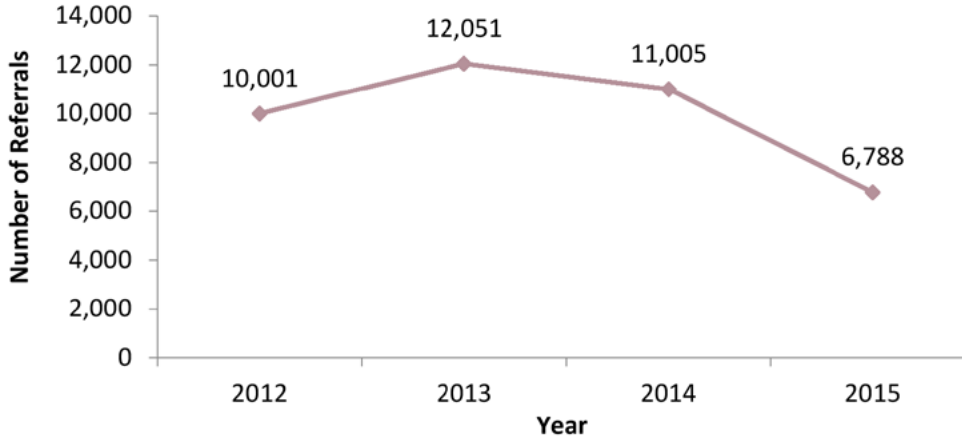
Mandatory Declassification Review Requests Average Number of Days to Resolve Each Request
FY 2012 – FY 2015



Mandatory Declassification Review Requests Unresolved for Over One Year
FY 2012 – FY 2015

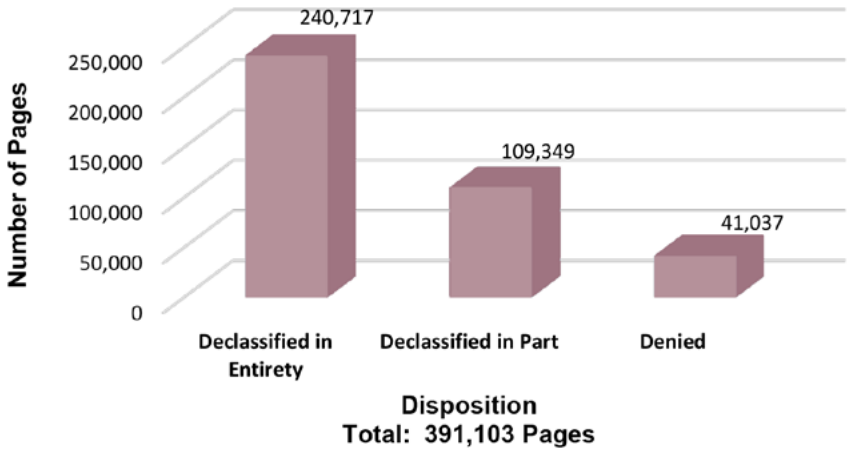


Mandatory Declassification Review Referred* Requests Received
FY 2012 – FY 2015

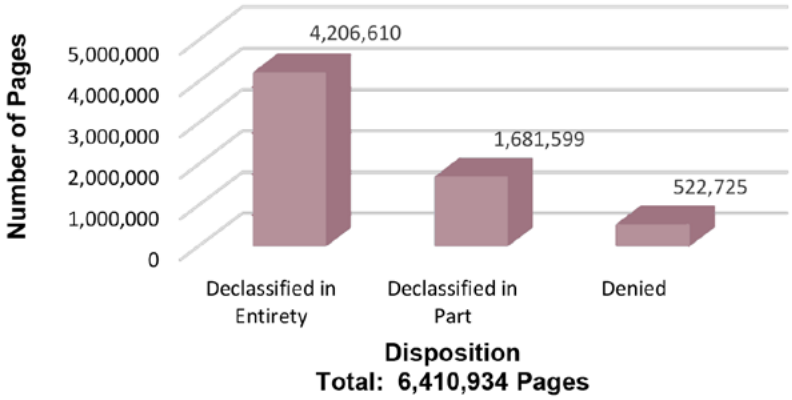


* MDRs referred to an agency from another agency that is responsible for the final release of the request.

Disposition of MDR Requests FY 2015

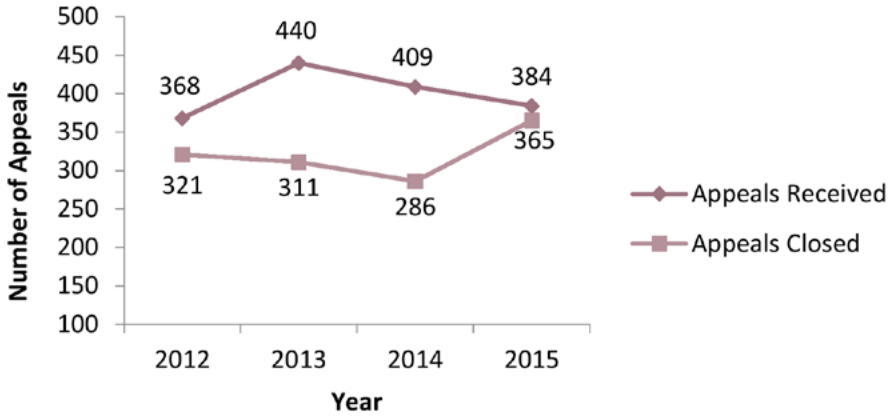


Disposition of MDR Requests FY 1996 – FY 2015

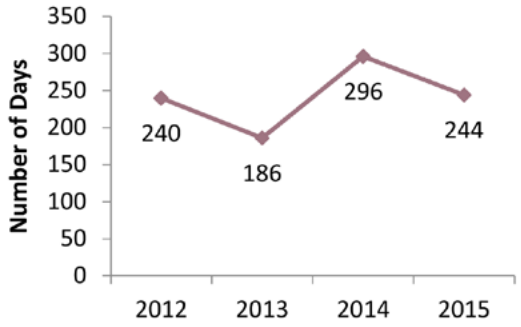


MDR Appeals

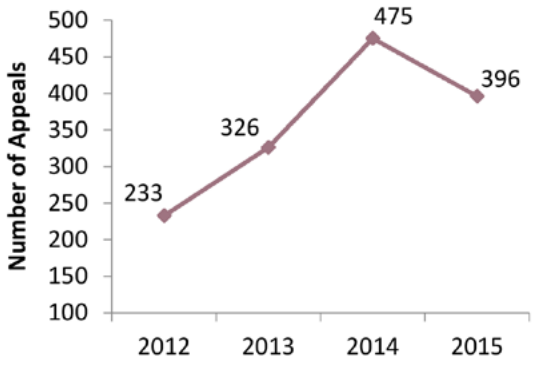
Mandatory Declassification Review Appeals
Received and Closed, FY 2012 – FY 2015



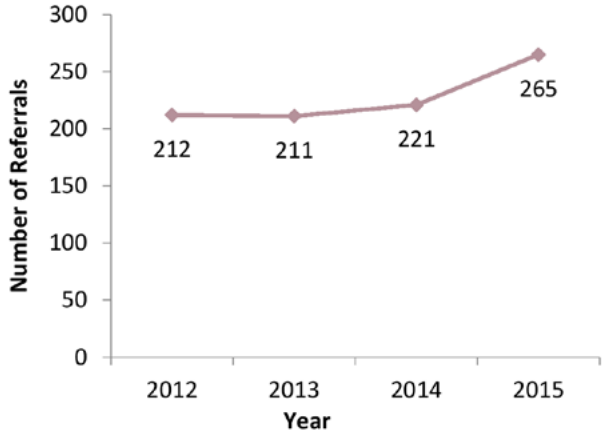
Mandatory Declassification Review Appeals Average Number
of Days to Resolve Each Appeal, FY 2012 – FY 2015



Mandatory Declassification Review Appeals Unresolved for
Over One Year, FY 2012 – FY 2015

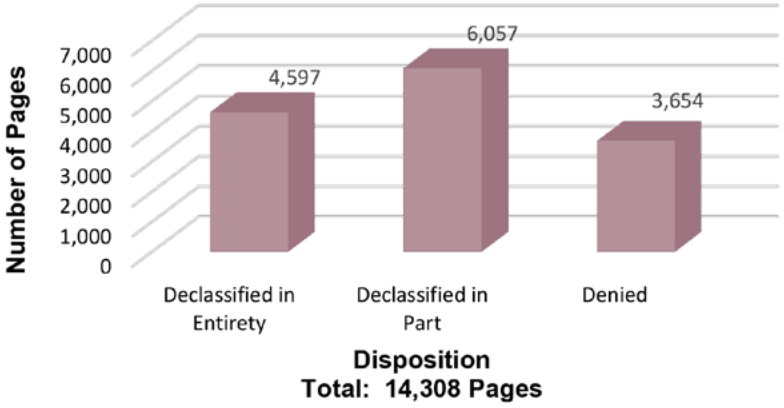


Mandatory Declassification Review Appeals
Referred Appeals Received, FY 2012 – FY 2015

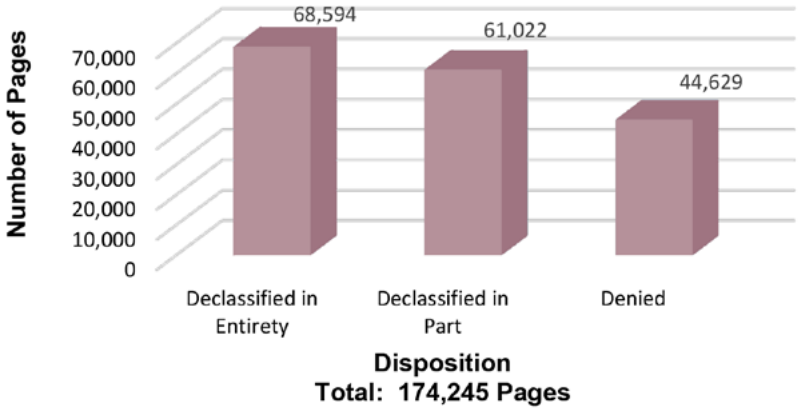


* MDRs referred to an agency from another agency that is responsible for the final release of the request.

Disposition of Mandatory Declassification Review Appeals, FY 2015



Disposition of Mandatory Declassification Review Appeals, FY 1996 – FY 2015



REVIEWS

Declassification Assessments

In FY 2015, ISOO conducted declassification proficiency assessments of six 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 on an annual basis at least 25 percent of agencies who 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, and six in FY 2015.

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

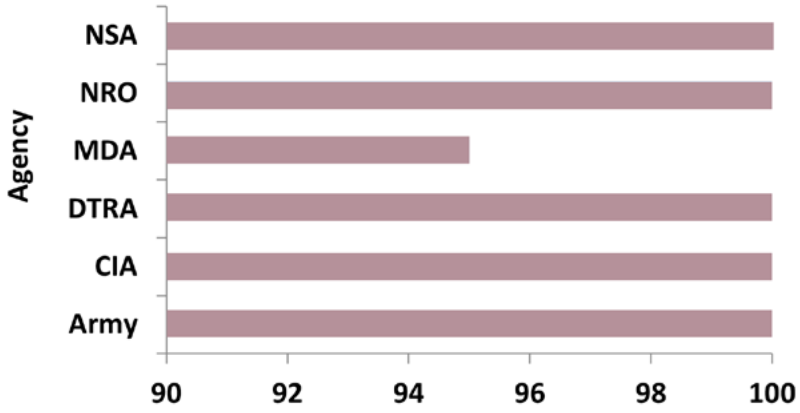
- Missed equities indicate instances of a declassification review not identifying for referral the security classification interest of one agency found in the record of another agency;
- Improper exemptions indicate instances of a declassification review resulting in the attempt to exempt a record from automatic declassification under an exemption category not permitted by that agency's declassification guide as approved by the Interagency Security Classification Appeals Panel;
- Improper referrals indicate instances of a declassification review resulting in the referral of records to agencies lacking the authority to exempt information from declassification or waiving their interest in declassification.

ISOO bases the overall agency score for the assessment on the occurrence and extent of any of these three issues. In addition to these three main categories, ISOO verifies that agency declassification policies and practices comply with ISOO policy guidance and that they are designed and implemented appropriately to assist the 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 assessments of six agencies in FY 2015: Department of the Army, Central Intelligence Agency, Defense Threat Reduction Agency, Missile Defense Agency, National Reconnaissance Office, and National Security Agency. All five agencies received "high" scores. There were no improper exemptions or improper referrals. ISOO encountered one instance of missed equity in a record referred to another agency. Additionally, ISOO continues to note positive progress in policy and program implementation. 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.

In FY 2016, ISOO will continue to conduct annual declassification assessments of agencies not yet assessed in the FY 2013-2016 review cycle. It will continue to provide agency-specific training and issue notices to agencies in order to provide specific guidance on areas of concern.

Declassification Assessment Results, FY 2015



Declassification Assessment Results, FY 2008 – FY 2015

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

Self-Inspections

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

The senior agency official (SAO) is responsible for directing and administering the agency's self-inspection program. In order for SAOs to fulfill their responsibilities, agency self-inspection programs must be structured to provide 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 utilized; and (2) information gathered through the agency's self-inspection program, which must include a summary and assessment of the findings from the self-inspection program, specific information from the review of the agency's original and derivative classification actions; actions taken or planned to correct deficiencies; and best practices identified during self-inspections. To ensure that agencies cover key requirements of E.O. 13526, the reports must also answer questions relating to areas such as training, performance evaluations, and classification challenges.

This is the fifth year of required descriptive self-inspection reporting, and as we noted last year, agencies are providing responses in nearly all of the required areas. Self-inspection reports must include findings from the agency self-inspection programs in two ways: in narrative responses, which give agencies the latitude to provide 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. In nearly all of these areas agencies reported improvement in compliance from last year.

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

- **Initial Training.** All cleared agency personnel are required to receive initial training on basic security policies, principles, practices, and criminal, civil, and administrative penalties. (32 CFR 2001.70(d)(1))
    - 84.78 percent of the agencies reported that all of their cleared personnel received this training (a decline from the 91.3 percent that reported full compliance last year).
    - Although full compliance is expected, we also consider if agencies come close to meeting this requirement: 95.65 percent of the agencies report at least 90 percent compliance this year (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))
    - 52.17 percent of the agencies reported that 100 percent of their cleared personnel received this training (a slight improvement from 50.0 percent that reported full compliance last year).
    - 82.61 percent of the agencies reported at least 90 percent compliance this year (an improvement from 76.09 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))
    - 63.64 percent of the agencies reported that 100 percent of their OCAs received this training (an improvement from the 50.0 percent that reported full compliance last year).
    - 72.73 percent of the agencies reported at least 90 percent compliance this year (an improvement from 63.64 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))
    - 70.0 percent of the agencies reported that 100 percent of their derivative classifiers received this training (an improvement from the 63.89 percent that reported full compliance last year).
    - 87.5 percent of the agencies reported at least 90 percent compliance this year (an improvement from 80.56 percent 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))
    - 41.3 percent of the agencies report that 100 percent of the required personnel have this element (36.96 percent reported full compliance last year).
    - 50.0 percent of the agencies reported at least 90 percent compliance this year (compared to 47.83 percent last year).

  That only half of the agencies are approaching full compliance with an important requirement whose purpose is to hold personnel accountable for their work with classified information is cause for concern. The significance of this is compounded because some of the agencies that identified that they do not sufficiently meet this requirement did not report they were taking actions to correct the shortcoming.

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

- **OCA Delegations.** Delegations of original classification authority shall be limited to the minimum required to administer E.O. 13526. Agency heads are responsible for ensuring that designated

subordinate officials have a demonstrable and continuing need to exercise this authority. (E.O. 13526, Sec. 1.3(c)(1))

- 90.0 percent of the agencies with OCA reported that delegations are limited as required (80.0 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 (67.39 percent 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 95,394 documents were reviewed to evaluate the application of this requirement (a considerable decrease from the 287,446 last year).
  - Agencies reported that 76.78 percent of the documents meet this requirement (an increase from 71.42 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 85,685 documents were reviewed to evaluate the application of this requirement (a considerable decrease from the 179,650 last year).
  - Agencies reported that 68.98 percent of the documents meet this requirement (a slight increase from 66.86 percent last year).

- **National Industrial Security Program (NISP).** Several questions were added to the self-inspection report this year to determine if agencies were meeting the basic requirements under the NISP, which was established under E.O. 12829 to safeguard Federal Government classified information that is released to contractors, licensees, and grantees (hereinafter referred to as contractors) of the United States Government. The Secretary of Defense serves as Executive Agent for inspecting and monitoring the contractors who require or will require access to, or who store or will store, classified information, and for determining the eligibility for access to classified information by contractors and their respective employees. Besides the Department of Defense (DoD), there are four other agencies that are Cognizant Security Agencies (CSA): the Office of the Director of National Intelligence (ODNI), the Department of Energy, the Nuclear Regulatory Commission, and the Department of Homeland Security, that are authorized to provide operational oversight of their contractors. The heads of other agencies, except the Central Intelligence Agency (CIA), are required to enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on behalf of these agency heads. The ODNI may enter into an agreement with the CIA authorizing the latter to inspect and monitor contractor programs

requiring access to intelligence sources and methods, including Sensitive Compartmented Information. Agencies with such contracts are also required to designate an SAO for the NISP and to provide classification guidance and security requirements to their contractors.

Agencies were asked to indicate if they had engaged in contracts that require contractors to have access to classified information. Those agencies that have such contracts were asked if they were meeting fundamental requirements of the NISP: if they entered into agreements with the Secretary of Defense for industrial security services, if the agency head has designated an SAO for the NISP, if the agency provides the contractor(s) current security classification guidance, and if the agency issued security requirements for the contractor(s) through either a specific contract clause or by a Contract Security Classification Specification (DD-254). On the self-inspection reports, 56.5 percent of the agencies indicated that they have engaged in classified contracts, but we know of several others that have such contracts.

- Of the agencies that indicated they have classified contracts and are not CSAs, 85.7 percent reported that they have entered into agreements with the DoD for industrial security services.
- Of the agencies that indicated they have classified contracts, 74 percent reported that the head of the agency has designated an SAO for the NISP.
- Of the agencies that indicated they have classified contracts, 81.5 percent reported that they provide the contractor current security classification guidance.
- Of the agencies that indicated they have classified contracts, 88.9 percent reported that they have issued security requirements for the contractor through either a specific contract clause or by a Contract Security Classification Specification (DD-254).

ISOO has begun to follow up with the agencies that did not report that they comply with these requirements of the NISP to determine if they indeed are not meeting the requirements or if they did not understand the new self-inspection reporting requirement.

There were improvements since last year in most of the areas outlined above, but there are still many agencies that have not reached an acceptable level of compliance in these areas. Of particular concern is that many of the agencies are not reporting actions to correct deficiencies that they identify in their reports. Nearly 24 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 19.6 percent of them outlined corrective actions for some but not all of the deficiencies they reported. In total, 43.5 percent of the agencies do not report that they are taking steps to correct all of the program weaknesses they identified. The most frequently reported deficiency for which no corrective action was provided is 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 utilize what they learn about their CNSI programs to manage and improve those programs.

Although some agencies are not making full use of the information they gather during self-inspections, there remains reason to be optimistic. In the decade prior to the issuance of E.O. 13526 with its requirement for detailed self-inspection reporting, ISOO on-site reviews found that a third of the agencies it visited had no self-inspection programs and

another third had very weak self-inspection programs. This has changed, and agencies now report that they do have self-inspection programs. We see in agency self-inspection reports and confirm during on-site reviews that some agencies' self-inspection programs are very strong. We will continue to work with the other agencies to help them improve their self-inspection programs.

Classified National Security Information Program Reviews

In FY 2015, pursuant to sections 5.2(b)(2) and (4) of E.O. 13526, ISOO conducted nine on-site reviews of executive branch agencies to evaluate the agencies' implementation of the classified national security information (CNSI) program. The reviews covered core program elements, such as program organization and management, classification and marking, security education and training, self-inspections, security violation procedures, safeguarding practices, and information systems security. Three of the agencies had strong CNSI programs, but at all of the agencies, including these, there were program areas that required attention in order to meet the requirements of E.O. 13526. 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, there were weaknesses in implementing regulations and performance evaluations. Section 5.4(d)(2) of E.O. 13526 requires agencies to promulgate implementing regulations. At three of the agencies, the implementing regulations reference E.O. 12958, which was effectively superseded by E.O. 13526 in June of 2010. At four agencies, although the implementing regulations satisfactorily cover the majority of the requirements of E.O. 13526 and 32 CFR part 2001, there are several omissions and a number of items that require revision. 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 security personnel have the required rating elements, while the majority of the personnel in the above categories are not evaluated. At five agencies, the performance plans cover only the management of classified information, not its designation. "Designation" was explicitly spelled out when E.O. 13526 was issued in December of 2009 because of the importance of accurate classification and marking of classified information. It is of serious concern that more than five years after the effective date of E.O. 13526 only two of the nine agencies ISOO reviewed had fully compliant implementing regulations. Likewise, it is most disappointing that only three of the nine agencies were fully compliant with the aforementioned performance evaluation rating requirement.

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 2001.15(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 three agencies lacked one or more of these elements. 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 in over ten years. Section 2001.15(b)(9)(ii) of 32 CFR part 2001 allows the use of the "25X" exemption codes as a declassification instruction in a security classification guide provided that (1) the exemption has been approved by the Interagency Security Classification Appeals Panel (ISCAP) under section 3.3(j) of E.O. 13526; (2) the ISCAP is notified of the intent to take such actions for specific information in advance of approval and the information remains in active use; and (3) the exemption code is accompanied with a declassification date or event that has been approved by the ISCAP. One agency had incorporated 25X exemptions into several classification guides but had not notified the ISCAP of its intent to take such actions. It is disconcerting that the majority of the nine agencies reviewed were not fully compliant with the completeness/accuracy/currency of their security classification guides, a fundamental tool to facilitate proper and uniform derivative classification of information.

At one agency, we noted a best practice for the regular and frequent review of classification guides. An agency component that has a research function routinely reviews the viability of its projects and in the process, reviews its classification guides as frequently as every six months. This is the strongest commitment to providing the most accurate and current classification guidance that we have seen in the executive branch.

ISOO reviewed a total of 1,184 classified documents at the nine agencies and identified marking discrepancies in 582 (49.2 percent) documents, finding a total of 836 document marking errors. At two of the agencies, more than 70 percent of the documents contained discrepancies, and two agencies had discrepancies in 60 percent of their documents. Marking discrepancies are more than just an administrative concern. The proper marking of classified materials is essential to demonstrate that information has been properly classified, to identify the individual who performed the classification action, and to communicate the period of time for which the information must be protected in the interest of national security. Proper marking 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.

Another significant issue that arose with the document reviews was the inability of three agencies to provide a sufficient sample of documents for ISOO to review. During on-site reviews, ISOO typically reviews a sample of 200 documents that were generated by the agency during the two years prior to the review. The sample should represent the classification activity of the agency by office, type of document, and classification level. Although the three agencies reported on their SF 311 classification activity during the two-year period at 35 to 170 times the requested sample size, none could provide more than 50 percent of the requested sample. It was unclear if the agency-reported SF 311 classification numbers were incorrect or if the agency security personnel were unable to gain access to documents.

Either scenario is problematic for internal agency oversight as one suggests that the security personnel do not understand where classification activity is taking place and the other indicates that classified materials might not be accessible for review in the agencies' self-inspection programs.

In the area of security education and training, the majority of the agencies ISOO reviewed had deficiencies. An effective security education and training program can only be achieved in an environment where all required knowledge is provided and where training results reach the performance level. At two agencies, not all personnel who derivatively classify had taken the training. At four agencies, the training did not address all of the topics required by 32 CFR 2001.71(d). One agency was not providing specialized training to its security personnel. All nine agencies provided the other forms of training required by E.O. 13526 and 32 CFR part 2001, but some did not cover all of the topics that 32 CFR part 2001 requires: in initial training, one agency did not cover some topics specified by section 2001.71(b); in training for OCAs, one agency did not meet the requirements of section 2001.71(c); and in refresher training, two agencies did not cover some of the topics outlined in section 2001.71(f). Also of concern were three agencies, which despite having strong security education and training programs, had personnel who displayed a lack of understanding of basic classification principles, such as the difference between original and derivative classification or the use of security classification guides.

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. One agency did not include a review of classified documents in its self-inspections. Two agencies, though reviewing documents, were not making a thorough assessment of their classification and marking. The document review should determine if any of the documents contain any of the discrepancies that are outlined in Part H of ISOO's Agency Annual Self-Inspection Data Form, to include over-classification, over/undergraded, declassification, duration, unauthorized classifier, "classified by" line, "reason" line, "derived from" line, multiple sources, marking, portion marking, and misapplication of a classification guide. The reviewers must have sufficient expertise to conduct the document review. An agency that performs a thorough and credible review of its classified product in both hard copy and electronic formats can identify strengths and weaknesses in classification and marking and can take steps through training and program enhancements to improve its program and products.

The information systems element of the ISOO on-site reviews focuses on the agencies' readiness and ability to protect classified information in accordance with applicable national policy. Federal departments and agencies must manage security risks against their classified information systems in order to combat the increasing number of internal and external threats that can never be completely eliminated but can be mitigated through shared measures and safeguards to protect such systems. Regulatory requirements for government classified information systems security focus on certifying and accrediting the security of information systems before putting them into operation. One major federal initiative is the transition from a static, paperwork-driven security authorization process to a dynamic framework that can provide authorization officials with on-demand access to security-related information to make risk-based decisions. Many agencies utilize a proactive approach to process reform that is aligned with the Office of Management and Budget guidelines that call on agencies and departments to provide real-time information about the state of their systems and networks. These efforts have resulted in security improvements, and the majority of

the agencies ISOO reviewed have very good information systems security programs.

Most agencies and departments have taken actions to address requirements related to education and training for users of classified information systems. A particularly notable best practice found at one agency is the implementation of a centralized system that tracks and reports personnel fulfillment of the initial and annual information systems security awareness training. For cases in which a user fails to complete training within the prescribed time, the system automatically restricts access to network resources by redirecting user logon to the training portal. This practice not only guarantees 100 percent training compliance; it also reduces the administrative burden.

In addition to these positive observations, the reviews found deficiencies and inconsistencies in assessment and authorization programs at some agencies. Requirements for securing information systems had not been fully implemented, and some agencies had not established sufficient oversight and communication to support their information systems programs. Specifically, key aspects of a successful program were not developed or maintained at some agencies. For example, some standalone computers that store, process, or transmit classified national security information lack formal authorization from an appropriate authorizing official. In some instances, no evidence was found of the existence of a follow-up mechanism for conditional approvals to operate. Additionally, portions of the information systems assessment and authorization documentation were missing or expired.

In FY 2016, ISOO will continue its broad on-site program reviews. We will also begin follow-up reviews of agencies where on-site reviews were conducted in FY 2014 to verify and validate agency corrective actions to address observations and recommendations from previous ISOO on-site reviews. The follow-up reviews will be limited to those program elements for which corrective actions were needed after the previous ISOO on-site review and will include a review of a smaller sample of classified documents than is performed on a full on-site review.

INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

Background

The President created the Interagency Security Classification Appeals Panel (ISCAP) (hereafter referred to as the Panel) by executive order in 1995 to perform the functions noted below. The Panel first met in May 1996. The permanent membership is comprised of senior-level representatives appointed by the Secretaries of State and Defense, the Attorney General, the Director of National Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs. The President selects the Chairperson. The Director of the Information Security Oversight Office serves as its Executive Secretary. ISOO provides staff support to Panel operations.

Authority

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

Functions

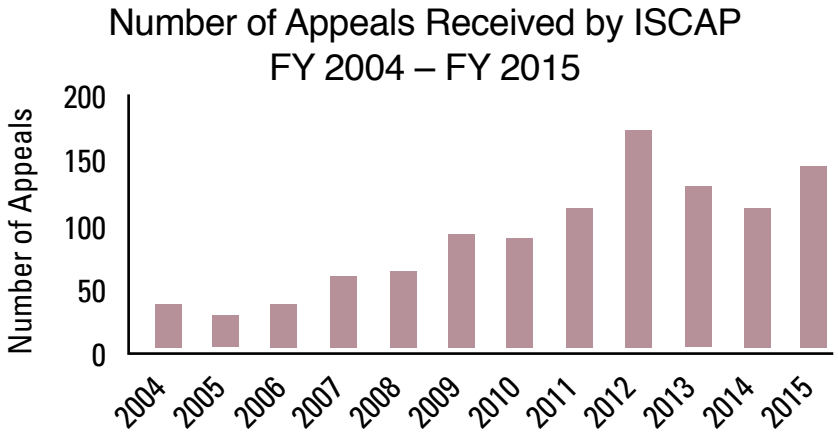
Section 5.3(b)

(1) To decide on appeals by persons who have filed classification challenges under section 1.8 of E.O. 13526.

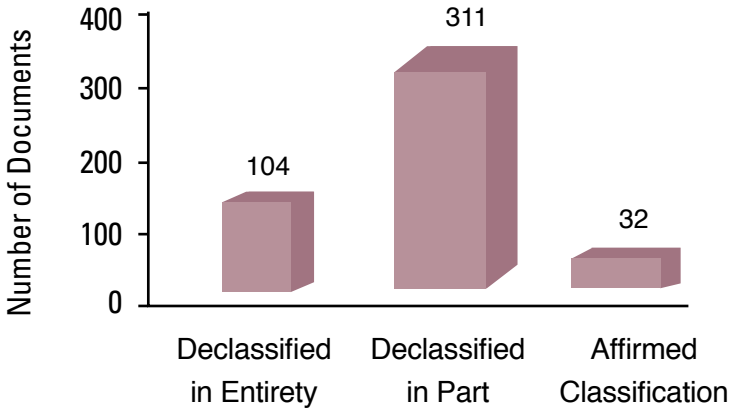
(2) To approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of E.O. 13526.

(3) To decide on appeals by persons or entities who have filed requests for mandatory declassification review (MDR) under section 3.5 of E.O. 13526.

(4) To appropriately inform senior agency officials and the public of final Interagency Security Classification Appeals Panel (the Panel) decisions on appeals under sections 1.8 and 3.5 of E.O. 13526.

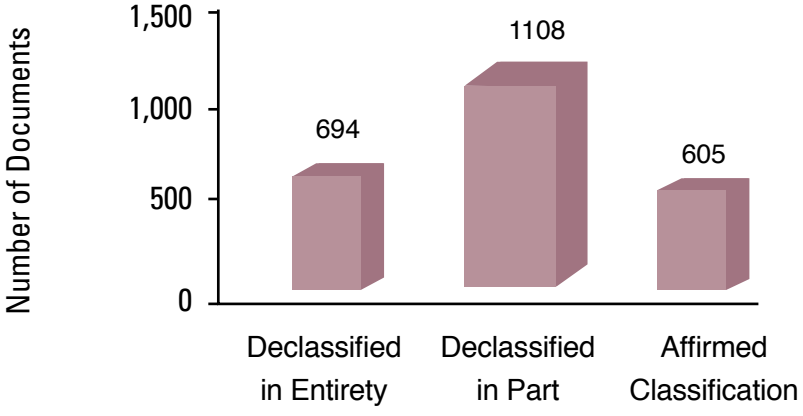


ISCAP Decisions, FY 2015



Total: 447 Documents

ISCAP Decisions, May 1996 – September 2015



Total: 2,407 Documents

Mandatory Declassification Review (MDR) Appeals

During FY 2015, the Panel continued to allocate a significant portion of its time and resources to processing MDR appeals. Appellants properly filed MDR appeals with the Panel in accordance with E.O. 13526 and the Panel's bylaws, 32 CFR part 2003. The Panel decided upon 55 MDR appeals, containing a total of 447 documents, including four motion picture recordings. The documents within these MDR appeals were classified either in part or in their entirety. The Panel affirmed the prior agency classification decisions in 32 documents (7 percent), declassified 104 documents (23 percent) in their entirety, and declassified 311 documents (70 percent) in part.

Since May 1996, the Panel has acted on a total of 2,407 documents. Of these, the Panel declassified additional information in 75 percent of the documents. Specifically, the Panel declassified 694 documents (29 percent) in their entirety, declassified 1,108 documents (46 percent) in part, and fully affirmed the declassification decisions of agencies in 605 documents (25 percent).

Classification Challenge Appeals

During FY 2015, the Panel 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. The next cycle of declassification guide review and approval by the ISCAP will begin in 2017. Each agency whose existing declassification guide was approved in 2012 must submit a revised declassification guide to the ISCAP by December 31, 2016. ISOO published the updated listing of agencies eligible to exempt information at 25, 50, and 75 years as ISOO Notice 2015-05.

ISCAP Decisions Website

In September 2012, the ISCAP Staff created a new website displaying electronic versions of documents the Panel recently declassified for public use. Section 5.3(b)(4) of the Order requires that the Panel "appropriately inform senior agency officials and the public of final Panel decisions on appeals under sections 1.8 and 3.5 of this order." This requirement is important for two reasons. First, the Panel adjudicates classification challenges and mandatory declassification review appeals that may be of historical interest to the public, not just the appellants. Second, section 3.1(i) of the Order states that, "When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel." Distribution of electronic versions of declassified documents on a publicly available website is the most efficient way for the Panel to provide senior agency officials (and agency declassification staffs) and the public with its decisions and fulfill this requirement. The Panel continued to add to and refine its listing of released documents during FY 2015.

ISCAP Appeals Status Log

In accordance with the spirit of the President's Open Government National Action Plan, 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. The ISCAP staff also posts information about status categories and about the process of appeal prioritization for ISCAP review.

ISCAP Members*

John W. Ficklin, Chair
National Security Council Staff

Garry P. Reid
Department of Defense

Mark A. Bradley
Department of Justice

Margaret P. Grafeld
Department of State

Sheryl J. Shenberger
National Archives and Records Administration
Jennifer L. Hudson
Office of the Director of National Intelligence

Executive Secretary
John P. Fitzpatrick, Director
Information Security Oversight Office

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

Support Staff
Information Security Oversight Office
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 this section were in these positions as of the end of FY 2015.*

Japanese Cabinet Minister Masako Mori met with the Archivist of the United States David Ferriero to learn about the functions of the Information Security Oversight Office (ISOO) and the Interagency Security Classification Appeals Panel. The Japanese Government has established an office similar to ISOO office as a result of the visit.

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 2015 is $16.17 billion. This includes the cost estimates of the Intelligence Community (IC)*, which total $2.06 billion. The IC costs comprise 12.8 percent of the total Government costs.

For FY 2015, agencies reported $1.95 billion in estimated costs associated with Personnel Security, an increase of $457.3 million, or 31 percent. The majority of this increase is attributed to an increased cost of periodic security clearance reinvestigations.

Estimated costs associated with Physical Security were $2.32 billion, an increase of $117.42 million, or 5 percent. Increased costs were due primarily to purchase and installation of security equipment and construction of secure facilities.

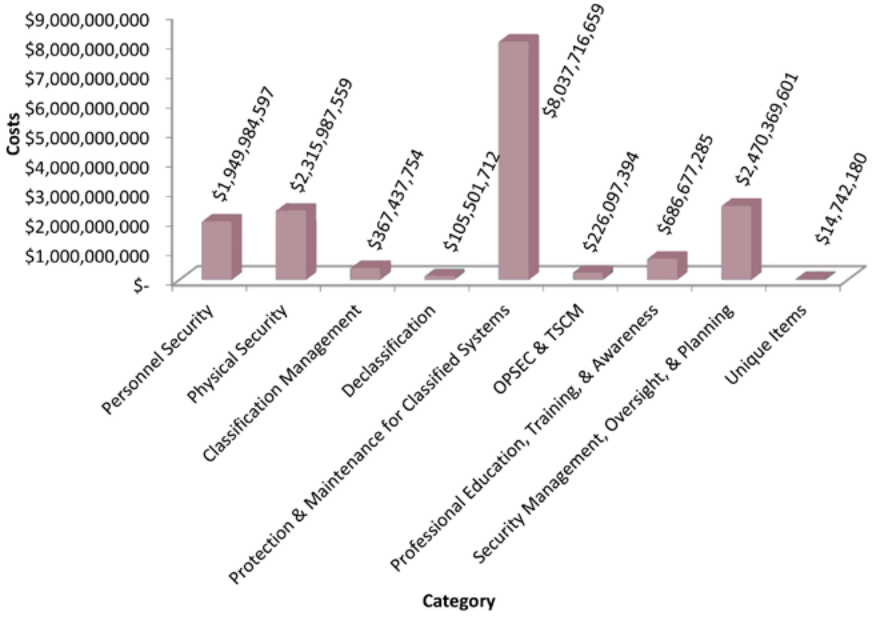
Estimated costs associated with Classification Management were $367.44 million, a decrease of $8.68 million, or 2 percent.

Estimated costs associated with Declassification were $105.50 million, an increase of $3.54 million, or 3 percent.

Estimated costs associated with Protection and Maintenance for Classified Information Systems were $8.04 billion, an increase of $469.28 million, or 6 percent. This increase can be attributed to a number of factors: improved reporting procedures, purchase and installation of classified systems, increase in maintenance costs, and the addition of a Crisis Management System.

Estimated costs associated with OPSEC and TSCM were $226.10 million, an increase of $52.20 million, or 30 percent.

Government Security Classification Costs
FY 2015



The estimated costs for Professional Education, Training, and Awareness were $686.68 million, an increase of $57.89 million, or 9 percent.

Estimated costs associated with Security Management, Oversight, and Planning were $2.47 billion, an increase of $48.51 million, or 2 percent.

Estimated costs associated with Unique Items were $14.74 million, a decrease of $2.88 million, or 16 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*

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 2015, the Defense Security Service collected industry cost data and provided the estimate to ISOO.

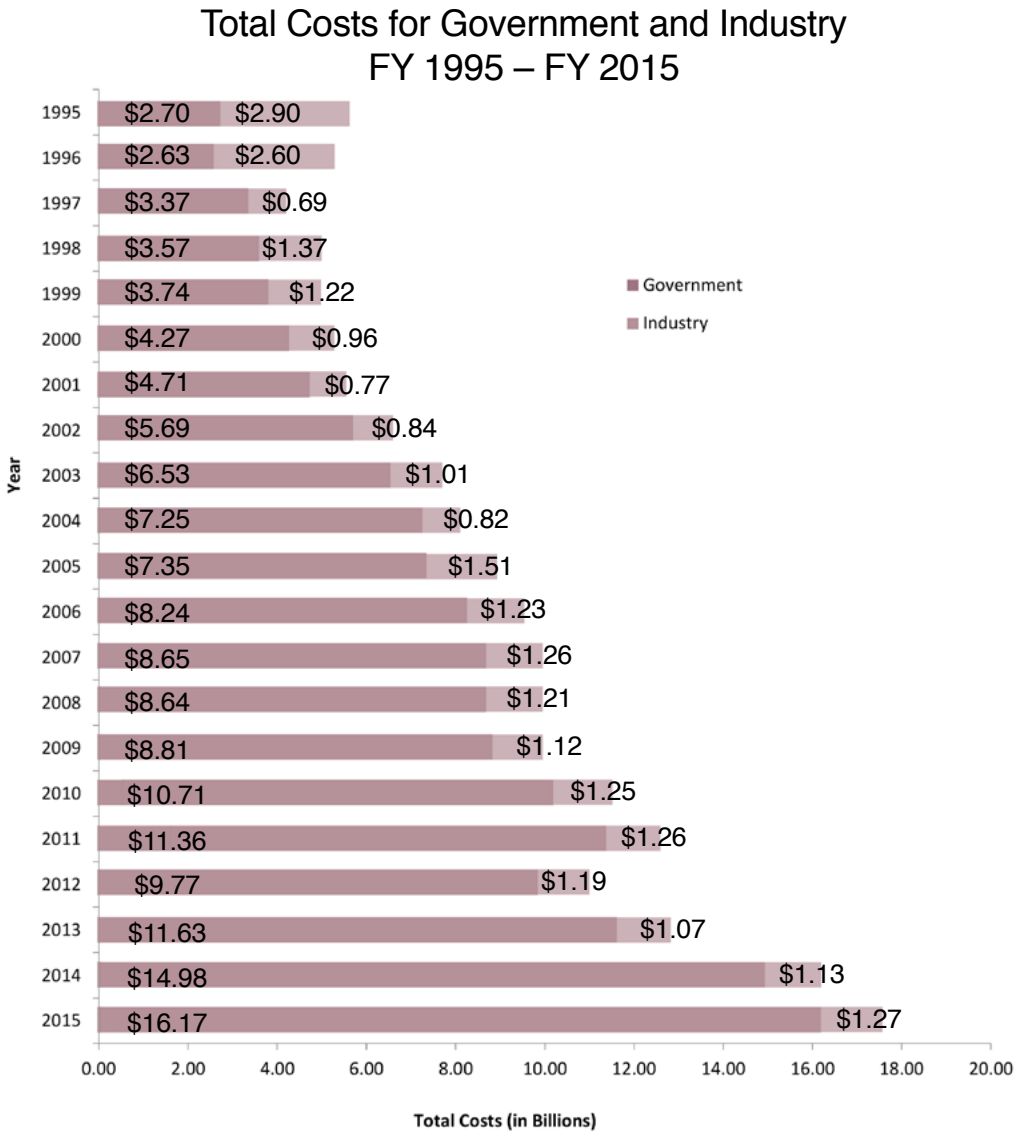
Cost estimate data are not provided by category because industry accounts for its costs differently than Government. Rather, a sampling method was applied that included volunteer companies from four different categories of facilities. The category of facility is based on the complexity of security requirements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

The FY 2015 cost estimate totals for industry per-

tain 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 2015 within industry was $1.27 billion; an increase of $136.25 million, or 12 percent.

Results—Combined Government and Industry

This year's combined estimate for Government and industry was $17.44 billion, an increase of $1.33 billion, or 8 percent.



NATIONAL INDUSTRIAL SECURITY PROGRAM

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

The NISPPAC advises on all matters involving the policies of the NISP and is responsible for recommending changes to industrial security policy, specifically E.O. 12829, as amended; its implementing directive, 32 CFR part 2004; and the National Industrial Security Program Operating Manual (NISPOM). The NISPPAC is required to convene at least twice during each 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 2015. The major issues discussed during these meetings included the timeliness of processing contactor personnel security clearances, the certification and accreditation of information systems processing classified information, industry implementation of national insider threat policies, national cyber security initiatives and the revision of the NISPOM and 32 CFR part 2004, NISP Directive No.1, to incorporate required changes.

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

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

Likewise, the Certification and Accreditation (C&A) of information systems working group continued its review and analysis of the processes for approval of contractors, grantees, and licensees of the Federal Agencies to process classified information on designated systems. This group continues to recommend changes to policies and standards, and tracks performance metrics to monitor the consistency, timeliness, and effectiveness of the C&A processes.

The issuance of government policy regarding insider threat created a need to revise portions of the NISPOM. To maximize the effectiveness of this rewrite effort, the NISPPAC working with DoD, as the NISP execu-

tive agent, the Cognizant Security Agencies (CSA), and other affected agencies, was provided an opportunity to review and recommend revisions to existing guidelines and proposed changes. A conforming change that will implement insider threat in the current NISPOM will be issued in FY 2016, and a comprehensive updated NISPOM is expected to be issued in FY 2018.

The continued emphasis on the sharing of information with non-NISP industry along with heightened concerns related to the confidentiality, integrity, availability, and resiliency of the nation's critical infrastructure among other things, resulted in the promulgation of Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," in FY 2015. This Order amended the NISP Order by adding the Department of Homeland Security (DHS) as the fifth CSA pursuant to their authorities under the critical infrastructure protection program. It also gave the Secretary of Homeland Security the authority to determine the eligibility for access to classified information of contractors, licensees, and grantees and their respective employees under a designated critical infrastructure protection program, including parties to agreements with such program. As a result, ISOO, DoD, and DHS jointly produced a hybrid approach to the facility security clearance vetting process for this subset of future NISP contractors that will not have authority to store classified information. Also, as part of the comprehensive update to the NISPOM, the DHS Secretary shall issue that portion of the Manual that pertains to classified information shared under a designated critical infrastructure protection program.

The impact of the implementation of the 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 2015, 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

The Controlled Unclassified Information (CUI) program was established by Executive Order 13556, "Controlled Unclassified Information" (the Order). The CUI program is intended to standardize the way the executive branch handles Sensitive But Unclassified (SBU) information, and to emphasize and enhance the openness, transparency, and uniformity of government-wide practices. ISOO manages the CUI program and fulfills the Executive Agent (EA) responsibilities designated by the Order to the National Archives and Records Administration (NARA).

Following issuance of the Order, Federal agencies reviewed their respective SBU information practices and submitted to the EA those categories and subcategories that the agency would like to continue to employ. The EA reviewed more than 2,200 proposed category and subcategory submissions, and worked with federal agencies to consolidate redundancies and provide consistency among like categories to build the baseline CUI Registry.

Policy Development

32 CFR part 2002

During FY 2015, the EA continued its iterative policy development strategy to incorporate uniform CUI policies and practices into the Code of Federal Regulations (CFR). This strategy included CUI Advisory Council (the Council) meetings, working group discussions, surveys and consolidation of current practices, analysis of current procedures, policy drafting, agency comments, public comments, and EA comment adjudication. The initial comment round of the process generated more than 800 comments from nearly 30 executive branch agencies. Adjudication of these comments reiterated the challenge of developing and coordinating a policy across the executive branch that addresses the broad spectrum of information types identified as CUI, and the wide range of capabilities, missions, and resources that exist throughout the Federal enterprise.

Based on the initial round of agency comment, NARA published a proposed regulation under 32 CFR part 2002, *Controlled Unclassified Information,* in the Federal Register (FR) on May 8, 2015 (80 FR 26501). During a 60-day public comment period, more than 245 individual written comments in addition to phone calls, email questions, and requests for information or clarification, were received from individuals, contractors, businesses, non-government organizations, academic and research organizations, state organizations, Federal agencies, and members of Congress.

Concurrent with the public comment period, on May 28, 2015, the EA hosted an open house for all Federal agencies to discuss the proposed regulation and its implementation. Regular meetings with the Council and subject-specific working groups throughout FY 2015 provided additional opportunities for discussion and input to policy development.

In September 2015, the EA, in consultation with the NARA Strategy and Communications Office, submitted a revised regulation and consolidated results of all comment adjudications to the Office of Management and Budget (OMB). The comment and adjudication process is anticipated to be brought to a conclusion in the coming months. Issuance of finalized 32 CFR part 2002 is projected for FY 2016.

National Institute of Standards and Technology Special Publication 800-171

Section 6a3 of the Order states that "This order shall be implemented in a manner consistent with…applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology (NIST), and applicable policies established by the Office of Management and Budget."

The protection of CUI while residing on non-Federal information systems and environments of operation is of paramount importance to agencies. Compromises of this information can directly impact the ability of the executive branch to successfully carry out its designated missions and business operations. Non-Federal organizations include contractors; state, local, and tribal governments; and colleges and universities.

During FY 2015, the EA collaborated with NIST and the Department of Defense (DoD) to develop NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. The NIST SP 800-171 was finalized and published in June 2015 and provides requirements for protecting the confidentiality of CUI that is held in non-federal systems and organizations. The guidelines apply to all components of non-federal information systems and organizations that process, store or transmit CUI, or provide security protection for those components.

Federal Acquisition Regulation

Upon finalization of the CUI Federal regulation, the EA will propose a single Federal Acquisition Regulation (FAR) rule that will apply the requirements of 32 CFR part 2002 and NIST SP 800-171 to the contractor environment. This will further promote standardization to benefit non-Federal organizations that may struggle to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from various agencies for the same information creates confusion and inefficiencies.

Until the formal process of establishing such a single FAR clause is complete, the NIST SP 800-171 may be referenced in a contract-specific requirement on a limited basis consistent with regulatory requirement. In FY 2015, the DoD modified the Defense Federal Acquisition Regulation (DFARS) 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting,* to require adequate security for all covered defense information on all non-federal information systems that support the performance of contract work, as per the requirements in NIST SP 800-171.

Policy Development Summary

The 32 CFR part 2002, NIST SP 800-171, and the CUI FAR rule will, in concert, provide agencies and non-Federal organizations with streamlined and uniform requirements for handling CUI.

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

The EA and CUI Advisory Council have defined Initial Operating Capability (IOC) as the ability to recognize CUI and to receive CUI for physical safeguarding. A target date for IOC will be established based upon publication of 32 CFR part 2002, and will be uniform across all agencies in the executive branch. Full Operating Capability will be achieved on an agency-by-agency basis, based on each agency completing all implementation tasks, including necessary information technology updates.

Training

To prepare for the publication of 32 CFR part 2002 and implementation of respective agency programs, the EA developed training toolkit aids to assist executive branch agencies with CUI awareness and communication rollout. Products developed include paper-based job aids, CUI implementation posters, and phased implementation charts of recommended agency-specific training activities. The EA will continue to conduct specialized workshops on CUI training to collaborate with impacted agencies, discuss implementation planning activities, and solicit input on training deliverables including draft training learning objectives.

Within six months of the issuance of 32 CFR part 2002, the EA plans to issue CUI baseline training modules. Each module will review key policy elements of the rule including, at a minimum, (1) safeguarding; (2) dissemination; (3) marking; and (4) decontrol procedures. Training modules will meet a range of technical specifications and will allow for tracking within agency learning management systems. In preparation, the EA began developing the framework of CUI baseline training modules and initiated testing of technical specifications previously collected from impacted agencies in an informal survey.

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

Oversight and Outreach

CUI oversight and outreach efforts are designed to assist executive branch agencies and departments in developing, implementing, and sustaining their respective CUI programs, and to offer advice, assistance, and guidance to non-Federal entities on core program elements.

In FY 2015, the EA continued its CUI program appraisal program for executive branch agencies to assist individual agency preparations for implementation of the CUI program. Appraisals are designed to be flexible and responsive to emerging developments and individual agency needs. Appraisals are scheduled based on agency request. Working with designated agency personnel, CUI staff members examine current policies, methods and practices used by a given agency to protect sensitive information. Key elements of focus include safeguarding practices, program management, training/awareness, self-inspections, system configuration, and incident/misuse remediation. Appraisal results and follow-up reviews provide agency planners with a baseline for developing implementation activities.

Standardized forms, templates, and electronic survey tools have been developed to streamline the appraisal process. Methods and materials used for the appraisals will be refined and adapted to monitor agency implementation and sustainment efforts as part of the EA's oversight responsibilities.

While conducting CUI program appraisals, an electronic survey of 25 questions is distributed to all agency employees, contractors, and detailees in order to establish a complete and accurate description of current operating

status regarding established policies, procedures, methods and practices surrounding the proper handling and protection of CUI. More than 3,100 surveys across 6 agencies were returned in FY 2015. Returns indicate that over 80 percent of respondents work in positions that require handling and protection of sensitive information, a finding that underscores the value of consistent practice. Collectively, appraisals conducted through FY 2014 and FY 2015 found that executive branch departments and agencies already incorporate many of the core elements necessary to implement the CUI program in accordance with standards and guidelines identified in the proposed 32 CFR part 2002.

Notable observations include:

- **Program Management.** All appraised agencies, departments, and components designate individuals to oversee certain aspects of information requiring protection. However, these officials may be dispersed throughout an organization, may receive operational authority from differing internal agency policies, and may not be obligated by policy to consult or notify other elements within the organization regarding their activities associated with the protection of sensitive information. ISOO recommends that these entities designate an agency focal point to ensure consistent implementation and to eliminate duplication of efforts.
- **Policy and Procedure.** All appraised agencies, departments, and components currently follow policies and procedures that prescribe protective measures for information that falls within the CUI program. Some policies and procedures call for the protection of information types that fall outside the program (i.e., protection measures not linked or linkable to a law, regulation, or Government-wide policy). Other policies fail to call for the protection of information that falls within the CUI program. Appraisals also identified gaps where agencies are protecting information that currently falls outside of the CUI program but where a reasonable need to protect the information exists. In such cases, agencies are advised to take appropriate steps to ensure adequate protections for the information and to ensure necessary protections are prescribed by the CUI program.
- **Training and Awareness.** All appraised agencies, departments, and components provide some level of training to their workforces on managing sensitive information. Most agencies currently deliver annual training to their respective workforces through a single Computer-Based Training module; other agencies use multiple on-line training modules. Common training topics include: (1) computer security, (2) personally identifiable information, (3) the agency's insider threat program, and (4) sensitive information as currently described by agency policy. Appraisals indicate that employees have a high degree of confidence in handling sensitive information. ISOO has recommended that agencies identify all internal training tools that currently address the protection or handling of sensitive information and, upon implementation of the CUI program, to update these tools as needed to address CUI program training concepts. ISOO also recommends that agencies consider consolidating and modifying existing training modules to reduce per-employee training cost and time.
- **Misuse and Incident Management.** All appraised agencies, departments, and components currently require that misuse in managing sensitive unclassified information be reported and mitigated. However, up to 40 percent of employees surveyed during FY 2015 were not aware of these requirements. Many agencies operate multiple incident reporting

systems, and program officials are not consistently informed of incidents and/or mitigation. ISOO recommends that agencies increase efforts to train their total workforces in incident and mitigation requirements. The EA suggests internal working groups as a potential mechanism to ensure proper notification across an agency of incidents involving sensitive information.

- **Self-Inspection.** Most agencies, departments, and components use self-inspection tools to evaluate existing practices for protecting sensitive information. These programs are designed to identify deficiencies and prescribe corrective measures. However, many appraised programs were found to focus on specific areas. ISOO recommends that agencies develop policies and procedures to evaluate the overall implementation of their respective CUI programs.
- **Information Technology Systems.** All appraised agencies, departments, and components can identify (1) the number of information technology systems used by the organization, (2) the configuration of each system as it relates to FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, and (3) whether or not systems process sensitive information. Most agencies assert that systems containing CUI are already configured to the standards identified in the proposed 32 CFR part 2002 (i.e., Moderate Confidentiality Impact Value) and that systems not configured to this standard (i.e., Low Confidentiality Impact Value) either do not process CUI or have already been designated for modification. ISOO encourages the continued development of implementation strategies related to information technology systems and recommends that, at minimum, agencies conduct internal assessments of information systems to (1) gauge their current configuration, in regard to the Moderate Confidentiality Impact Value, (2) assess whether or not systems contain CUI, as described by the CUI Registry, and (3) target systems that contain or process CUI and are currently configured below the Moderate Confidentiality Impact level for modification to the required standard within four years of the release of 32 CFR part 2002.

At the May 2015 ISOO Open House, the EA connected with more than 200 stakeholders face-to-face to advance awareness of the CUI program, its history and current status. During FY 2015, the EA conducted briefings and on-site training; participated in panel discussions; and provided consultation to over 30 executive branch agencies, and various industry and non-federal organizations. By leveraging available technology, ISOO extended briefing, training, and education to entities outside the immediate Washington, DC metro area.

CUI Registry and Website

As the repository for common definitions, protocols, and procedures for properly marking, safeguarding, disseminating, and decontrolling unclassified information, based on law, regulation, and government-wide policy, the CUI Registry is a central element of the CUI program. At the May 2015 ISOO Open House, CUI staff presented a workshop on the CUI Registry providing background, current status, and anticipated future functionality of this cornerstone of the CUI program to more than 200 representatives from over 30 agencies within the Federal government.

The online CUI Registry currently includes descriptions for 23 categories and 83 subcategories of unclassified information, supported by 315 unique control citations and 101 unique sanction citations in the United States Code (U.S.C.), CFR, and government-wide policies. All control and sanction authority references were reconfirmed and updated based on annual updates to the U.S.C. and CFR, and review of government-wide policy documents. During FY 2015, 15 citations for authorizing language moved from one section of the U.S.C. to another, either within an individual title, or to a different title of the Code. In these cases, the Registry was updated to reflect the new location of the authority language, but noting the previous section. Previous authority references will be retained for one update cycle.

The EA continues to update the CUI Registry based on identification of unclassified information that requires protection based on law, regulations, and/or government-wide policies. Changes to categories and subcategories are made in consultation with the CUI Advisory Council. Examples of FY 2015 Registry changes made with Council input included: (1) addition of categories and subcategories to the Registry; (2) update of category/subcategory names; and (3) consolidation of categories and/or subcategories. .

In addition to the online Registry, the CUI web presence provides updates, handouts, training modules, reports, and answers to frequently asked questions. The CUI portal was updated in FY 2015 to more distinctly delineate between elements of the CUI program. Providing clear and readily accessible direction will promote more consistent protection and sharing of sensitive information both internally and externally.

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

NATIONAL ARCHIVES

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