NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

2017 REPORT TO THE PRESIDENT

WASHINGTON, DC 20408-0001

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) resides within the Agency Services organization of the National Archives and Records Administration. ISOO 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 allows proper access to sensitive and classified information to advance the national and public interest. We lead efforts to standardize and assess the management of classified and controlled unclassified information (CUI) through oversight, policy development, guidance, education, and reporting.

FUNCTIONS

- Develop implementing directives and instructions.
- Review and approve agency implementing regulations and policies.
- Review requests for original classification authority and CUI categories from agencies.
- Maintain liaison relationships with agency counterparts and conduct on-site and document reviews to monitor agency compliance.
- Develop and disseminate security education materials for Government and industry; monitor security education and training programs.
- Receive and take action on complaints and suggestions regarding administration of programs established under E.O.s 13526 and 13556.
- Collect and analyze relevant statistical data and, along with other information, report annually to the President.
- Recommend policy changes concerning information security 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.
- Provide program and administrative support for the Public Interest Declassification Board.
- Serve as Executive Agent to implement the CUI program under E.O. 13556 and oversee agency actions.
- Chair the National Industrial Security Program Policy Advisory Committee 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 the 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 security classification and controlled unclassified programs.

LETTER TO THE PRESIDENT

May 31, 2018

The President of the United States
The White House
Washington, DC 20500

Dear Mr. President:

The security classification system plays a pivotal role in our national security. It supports military operations, intelligence activities, and diplomacy. Its performance, though, is facing increasing challenges. We can and must reduce costs and increase efficiency by using digital technology to replace existing analog and paper-based operations. Our system keeps expanding, but remains hamstrung by old practices and outdated technology. We are at a crossroads.

The Information Security Oversight Office (ISOO), under the authority of Executive Orders 13526, "Classified National Security Information," and 13556, "Controlled Unclassified Information," oversees both the Classified National Security Information (CNSI) and Controlled Unclassified Information (CUI) programs. Enclosed is ISOO's Report for Fiscal Year (FY) 2017. It depicts the current health and status of the security classification system and the implementation of the CUI program. It provides findings and recommendations that will improve and modernize both programs.

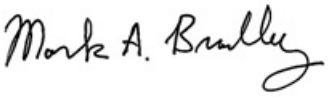
ISOO recommendations support modernizing the security classification system to transform how Government manages our classified information for the 21st century. Users of the system, both inside and outside the Government, agree that the current framework is unsustainable. Too much classification impedes the proper sharing of information necessary to respond to security threats, while too little declassification undermines the trust of the American people in their Government. Reforms will require adopting strategies that increase the precision and decrease the permissiveness of security classification decisions, improve the efficiency and effectiveness of declassification programs, and use modern technology in security classification programs across the Government.

The prohibitive cost of maintaining this outdated system continues to rise. ISOO estimates that in FY 2017 the Government alone spent $18.39 billion on security classification, while private companies spent another $1.49 billion to work with federal agencies under the National Industrial Security Program.

The full implementation of a robust CUI program designed to better protect and facilitate the sharing of sensitive information will further advance national security imperatives. This program's implementation, though, remains controversial and challenging. While many agencies have embraced its benefits, a sizeable number have given it only limited support and have been too sluggish in developing policies and practices to implement it. I believe the White House must strongly intervene to underscore the critical importance of the CUI Program's full implementation.

I believe these recommendations, if followed, will advance the national security of the United States. Thank you for reviewing and considering the recommendations in this report.

Sincerely,



Mark A. Bradley
Director
Information Security Oversight Office

TABLE OF CONTENTS

JUDGMENTS, KEY FINDINGS, AND HIGH PRIORITY RECOMMENDATIONS 1

CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI) PROGRAM 7

- CLASSIFICATION 8
  - Original Classification Activity 8
  - Derivative Classification Activity 9
  - Classification Challenges 11
  - Fundamental Classification Guidance Review (FCGR) 12
- DECLASSIFICATION 14
  - Automatic, Systematic, and Discretionary Review 14
  - Mandatory Declassification Review 16
- REVIEWS 19
  - Declassification Assessments 19
  - Self-Inspections 20
  - CNSI Program On-Site Reviews 23

INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL (ISCAP) 27

COST ESTIMATES FOR SECURITY CLASSIFICATION ACTIVITIES 29

NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) 31

CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM 34

- CUI IMPLEMENTATION 35

APPENDIX: REPORTED DATA 41

JUDGMENTS, KEY FINDINGS, AND HIGH PRIORITY RECOMMENDATIONS

Judgments:

- Information security has an increasingly critical function in Government operations. The complexities associated with information protection and sharing require information security play a more central role in agency mission objectives.
- The long-term sustainability of the security classification system depends largely on achieving strategic reforms in Government-wide policy and technology modernization.
- The White House, coupled with the support of senior agency leaders, must lead the charge in modernizing technology that underpins our country's security classification system.
- Reforms for modernizing the security classification system will require adopting strategies that increase the precision and decrease the permissiveness of security classification decisions, improve the efficiency and effectiveness of declassification programs, and use modern technology in security classification programs across the Government.
- Responsibilities for oversight and monitoring of the security classification system and the controlled unclassified system will continue trends of decentralization and dissemination, moving to a more collaborative assessment and reporting relationship between ISOO and agencies. Effective oversight of such wide-spread systems will require much stronger agency self-inspection programs.
- Information systems security will ascend as the leading core element of concern in oversight and monitoring of the security classification system.
- Without White House intervention to emphasize the need for top-level agency support and funding, CUI Program implementation will be significantly delayed. This leaves information protection and sharing for CUI in serious jeopardy.

Key Findings:

►Original classification decisions increased by 49% (58,501 decisions), yet still remained a small fraction of overall classification activity when compared to derivative classification (49 million decisions).

- Original classification authorities (OCA) decreased to a new low of 1,867 (16% decrease).
- Data demonstrated consistently that the number of OCAs at the Secret level remained significantly greater than that of the Top Secret or Confidential levels.
- The use of the "Ten Years or Less" declassification instruction continued to increase in use in original classification. The FY 2017 rate increased to 66%, up from 30% use in FY 2016 reporting.

- Derivative classification activity was reported by agencies through an estimation of overall agency activity. The accuracy of the figures continues to be difficult for ISOO to verify.
  - Derivative classification activity decreased for the first time in four years, to a total of over 49 million decisions, the lowest count since FY 2008.
    - It is unclear yet if this is an anomaly or the start of a new trend.
  - Derivative classification activity estimates demonstrate the fairly consistent trend of a significantly greater volume occurring at the Secret level than at either the Top Secret or Confidential levels.

►There were a total of 721 formal classification challenges, a decrease of 233 challenges, or 24% from FY 2016 reporting.

- The Department of Defense (DoD) reported 677 formal challenges. The "big six" Intelligence Community (IC) agencies (Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and Office of the Director of National Intelligence (ODNI)), reported a total of 3 formal classification challenges for FY 2017.
- The majority of the challenges made—638, or 88%—resulted in overall affirmation of the original classification decision.
- In 8% of the challenges, the classification decision was overturned in whole or in part (58 challenges).
- The remainder—4%—were closed for administrative reasons.
- Despite its limited use, the challenge provision provided an important mechanism for system self-regulation through the use of an impartial third-party review of classification actions.

►The Fundamental Classification Guidance Review (FCGR) resulted in more uniform and consistent guidance largely brought about by efforts to team Subject Matter Experts (SME) with program managers and technologists who were more actively engaged in the 2017 FCGR than during the 2012 FCGR.

- Agencies reported 2,865 security classification guides (SCG) reviewed, 221 SCGs cancelled, 533 SCGs consolidated, and 14 new SCGs written.
- The total number of active SCGs at the end of the review was 2,154.

►Declassification remained a resource-intensive, paper-based review process, unable to meet the demands imposed by the large volume of paper records in need of review. Agencies were unable to meet the demands of electronic records review.

- The total page count for declassification review decreased under automatic, systematic, and discretionary declassification programs by 18%.
- The systematic declassification rates decreased significantly, from 79% to 35%, attributable to the effects litigation from Freedom of Information Act (FOIA) requests had on resources devoted to declassification.
- Although both increased, automatic and discretionary declassification rates remained low at 55% and 38%, respectively.

►Agencies struggled to close Mandatory Declassification Review (MDR) requests and appeals, resulting in growing backlogs in need of processing.

- MDR requests and appeals continued providing higher declassification rates than automatic, systematic, and discretionary declassification review.

►On-site reviews of CNSI programs found agencies need to improve a variety of program elements, including the correct use of portion markings, declassification instructions, and documentation of the derivative classifier in markings.

- Follow-up reviews found agencies addressed only 39% of findings in an original on-site review.
- Agencies with fewer marking errors used marking tools and templates, had quality control processes, and comparatively more effective self-inspection programs that reviewed samples of classified documents consistently.

►Agency self-inspection reporting showed varying degrees of compliance and performance among agencies. Of concern, however, are the many agencies that reported an unacceptably low level of compliance with core CNSI program requirements, including training, performance evaluations, establishing classification challenge procedures, and applying marking requirements.

►The workload of the Interagency Security Classification Appeals Panel (ISCAP) increased and will continue to escalate dramatically.

- The 577 appeals received by the ISCAP in FY 2017 was the largest number of appeals ever received in any previous fiscal year.
- The yearly increase in appeals has led to an appeals backlog, which likely will continue to rise.
- This dramatic increase in appeals received was due in part to the capability for direct appeal to the ISCAP of MDR requests when an agency failed to provide a final response within one year.
- The increase was also attributable to the monopolization of very limited resources by a handful of appellants, as well as by the effects litigation from FOIA requests are having on agency declassification review programs.

►Agency CUI status reports illustrated the need for continuing oversight of agency CUI implementation efforts.

- ISOO received required annual reports from 61 of 136 agencies (45%), including all but two of the cabinet-level departments, the Departments of Commerce and Energy.
- 105 agencies reported appointing CUI Senior Agency Officials (SAO) and program managers.
- Reporting showed varying completion of CUI agency policies.
  - Six agencies reported issuing CUI implementing policies.
  - 11 agencies reported having policies under internal review and near finalization.

- 30 agencies reported having policies in development and projected for issuance in FY 2018.
- 12 agencies reported policies projected for issuance in FY 2019.

- Agencies used existing personnel and resources for all CUI implementation activities during FY 2017, which significantly impeded agency implementation efforts.

►Security classification costs continued to increase, totaling $18.39 billion in FY 2017, an increase of $1.5 billion from FY 2016 reporting (9%).

- Personnel security; physical security; protection and maintenance for classified systems; and security management, oversight, and planning remained the categories of greatest expense for Government, totaling in the billions of dollars in each of the four functions.
- The Defense Security Service (DSS) provided a total security classification cost estimate for cleared industry of $1.49 billion, an increase of almost 17%.

Recommendations:

Based on our judgments and key findings, ISOO provides the following recommendations supporting transformative change, which we understand will require a multi-faceted, multi-year effort to achieve. ISOO will work collaboratively with leadership at the National Security Council (NSC) and with agencies to consider, amend, prioritize, adopt, and implement actionable tasking items in support of chosen recommendations. Future ISOO Annual Reports to the President will address the steps needed to achieve agreed-upon strategic goals and objectives.

►Agencies are in need of a Government-wide technology strategy for the management of classified information to combat inaccurate classification and promote more timely declassification.

►The technology investment strategy must require agency budget requests include estimates for security classification costs. Doing this will advance the modernization of classification and declassification, as well as improve information systems security, which impacts the health of the security classification system.

- The Office of Management and Budget (OMB) should consider reforming the budget process to accommodate security classification as a line-item, as well as prioritize funds for research and development activities and transform acquisition practices.

►With cooperation from the NSC, OMB and ODNI, ISOO must develop a more effective way to measure and assess the health of the CNSI Program.

- **The technology investment strategy must include a requirement for agencies to implement new risk management approaches that stress mitigation rather than avoidance to assist in reducing costs, promote appropriate information sharing, and increase the efficiency of declassification.**

- **Policies must be revised to improve the effectiveness and efficiency of automatic declassification. Policy reforms need to address declassification's role in delaying access to high volumes of historically significant records and the impact it has on the volume of records awaiting further review at 50 years of age.**
  - Reforming automatic declassification will require addressing low release rates and exorbitant costs of analog processes in place at agencies.
  - Policies must be revised to limit the scope of records exempted from the application of automatic declassification under E.O. 13526. Agencies and the public must work collaboratively to determine how best to prioritize records for review given the limited resources available.

- **Ideally where technology and resources allow, agencies should strive to practice redaction review in lieu of pass-fail review methods.**

- **Agencies must address and modernize their information systems security, especially as related to its impact on the protection and sharing of controlled unclassified and classified information. Reforms are necessary for oversight programs to function in an increasingly decentralized framework supporting electronic records management.**

- **On-site CNSI review programs must transition from a broad assessment of the total of an agency's program to assessing and recommending specific, tactical program improvements that address areas of Government-wide concern.**

- **Agencies must meet requirements of E.O. 13526 concerning classification training, performance evaluation, and challenge procedures.**
  - All agencies must be at least 90% compliant with all training and performance evaluation categories.
  - All agencies must institute classification challenge procedures and include classification challenge procedures as part of their training and performance evaluation.

- **We intend to work with the ISCAP members to amend its bylaws in order to return to the original mandate of this Presidential appellate body - to decide on appeals concerning records of historical significance and of most interest to the public.**
  - Current policies and procedures permit very limited resources to be devoted to ISCAP appeals from a handful of serial appellants.
  - Amending the bylaws and E.O. 13526 by reforming automatic declassification, adjusting MDR deadlines, and reexamining declassification guide reviews will decrease the amount of records appealed to the ISCAP.

- **The ISCAP should recommend expanding its membership to include a member of the public (able to obtain the appropriate security clearances and willing to sign the necessary nondisclosure agreements) and to agencies with expanded and growing CNSI programs, such as the Department of Homeland Security (DHS). The role of the public citizen would be to garner support for any improvements the ISCAP adopts and would enhance sustained credibility in ISCAP decision-making activities.**

- **Agencies must move expeditiously to finalize their CUI program policies so that dependent core elements of implementation may proceed.**
  - Where not already done, agencies must appoint CUI SAOs and program managers to oversee the CUI Program in their agencies.
  - Policies must be revised to implement CUI Program requirements. Policy reforms need to identify the different categories of CUI the agency handles and set out agency practices necessary to meet all CUI requirements for those categories of information.
  - Agencies must implement CUI Program requirements for training, IT systems assessment, and self-inspection procedures.

- **Agencies must complete budget requests consistent with OMB Circular A-11, "Preparation, Submission, and Execution of the Budget," and submit cost estimates and projections as part of their CUI annual reports.**
  - Only with these annual report submissions can ISOO assess and oversee the status of implementation of the CUI Program across the executive branch.

CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI) PROGRAM

CLASSIFICATION

ORIGINAL CLASSIFICATION ACTIVITY

Authority:

E.O. 13526, "Classified National Security Information," Section 1.3.

Findings:

- Agencies reported 1,867 Original Classification Authorities (OCA) in FY 2017; a 16% decrease from the 2,215 OCAs reported in FY 2016.
  - Top Secret OCAs: 716.
  - Secret original OCAs: 1,114.
  - Confidential OCAs: 37.
- Agencies reported 58,501 original classification decisions for FY 2017, applying the "Ten Years or Less" declassification instruction in 66% of the decisions.
  - Top Secret original classification decisions: 1,398.
  - Secret original classification decisions: 48,056.
  - Confidential original classification decisions: 9,047.

Analysis:

Original classification activity remains one of the limited measures available that accurately reflects some amount of restraint being exercised on the application of security classification permitted by E.O. 13526. Unlike derivative classification estimates, the data reported describing original classification activity are more closely tracked and more exact. This is due in part to fewer practitioners of security classification having authority to perform original classification. This in turn contributes to a significantly smaller amount of original classification activity than derivative classification activity. Agencies self-regulate much of their original classification activity to a more stringent level than is possible with derivative classification activity.

The number of OCAs in FY 2017 decreased by 16%, continuing a consistent long-term trend in the reduction of OCAs across agencies. Data on the OCAs from FY 1998—FY 2017 show a consistent trend in the number of OCAs at the Secret classification level remaining significantly greater.

Original classification decisions increased for the first time in four years, to its highest level since FY 2013. Agencies reported 58,501 original classification decisions, an increase of 49%. Original classification decisions continued the long-standing trend of occurring at consistently greater frequency at the Secret level than at the Top Secret or Confidential levels. Agencies reported 48,056 original classification decisions at the Secret level, or 82%, which is an increase of 13% from FY 2016 reporting.

The significant increase in Secret level original classification decisions may reflect a growing imperative to classify originally at a level where greater information sharing is possible. Whether this increase represents an anomaly, or is the beginning of a new trend concerning information sharing, remains unclear.

The application of the "Ten Years Or Less" declassification instruction at the time of original classification is beginning an upward trend in its use, more than doubling from 30% application in FY 2016 to 66% application in FY 2017, likely due to cost considerations. Prolonging classification brings higher long-term costs associated with physical security and the protection and maintenance for classified systems.

Outcomes:

Our national security requires more precise and less permissive classification practices. The key lies in confining original classification decisions to the minimum necessary required to support mission objectives. Inaccurate classification activity—most often manifested in over-classification—presents a significant barrier to appropriate information protection and sharing.

The increasing costs of security classification also warrant more measured application of original classification. Cost considerations may also affect the trend toward greater original classification activity at the Secret level.

As it stands now, the security classification system operates as a de facto two-level system. Agencies follow two levels of information systems security, two levels of personnel security clearance, and two levels of physical safeguarding. Limited original classification activity at the Confidential level may support future migration to a two-level classification system, similar to what the British have successfully implemented.

DERIVATIVE CLASSIFICATION ACTIVITY

Authority:

E.O. 13526, "Classified National Security Information," Section 2.1.

Findings:

- Agencies reported an estimated total of over 49 million derivative classification decisions in FY 2017, a decrease of 10% from FY 2016.
    - Top Secret derivative classification activity: 9,615,440.
    - Secret derivative classification activity: 36,115,335.
    - Confidential derivative classification activity: 3,710,737.

Analysis:

Derivative classification decisions decreased for the first time in four years, to an estimate of just over 49 million decisions, the lowest estimated count since FY 2008. Whether this decrease represents an anomaly, or the start of a new trend, remains unclear. Estimates of derivative classification activity remain consistent with the trend of most activity occurring at the Secret level, in contrast to trends at the Top Secret and Confidential levels.

Count estimates reported by agencies grow increasingly difficult for ISOO to verify. Agencies are facing significant complexities and challenges associated with data reporting on information that is a hybrid of records in both paper and electronic format. Even with these challenges, ISOO has found many agencies remain fairly consistent in their internal agency methodology for measuring derivative classification activity estimates. A similar measure of derivative classification activity consistently reported over time does allow for the identification of some trends regarding the overall volume of derivative classification. These trends indicate that the volumes of information generated in the current digital information environment make the scalability of existing methodologies increasingly problematic.

Outcomes:

The prevailing high costs of derivative classification require the development of a more meaningful, data-driven methodology than what is currently employed to determine the appropriate volume and accuracy of derivative classification activity across the executive branch. Deciding whether the demands of proper information management warrant the current volume of derivative classification requires more accurate data regarding the volume and growth of information than agencies currently provide.

The basis for improving the precision of derivative classification lies in ensuring that accurate and measurable original classification occurs at the *minimum level necessary* to support mission objectives. Precise metrics describing derivative classification activity will assist in determining the prevalence of misclassification (e.g. over- and under-classification) and will help in developing a path toward correcting inaccuracies carried out by system users.

Until the Government adopts and implements a plan to modernize IT that will automate much of the classification activity occurring at agencies, misclassification will continue to challenge the proper functioning and credibility of the security classification system.

Modernizing reporting processes will require collaboration across the executive branch that deeply involves experts in cybersecurity and the security of information systems crucial to safeguarding and information sharing programs.

CLASSIFICATION CHALLENGES

Authority:

E.O. 13526, "Classified National Security Information," Section 1.8 (b).

Findings:

- Formal classification challenges: 721.
  - Fully affirmed at their current classification status: 638.
  - Overturned either in whole or in part: 58.
  - Administratively closed: 25.
- Self-inspection reporting revealed 76% of agencies have established formalized procedures for classification challenges, which is identical to FY 2016 reported findings.

Analysis:

There were a total of 721 formal classification challenges in FY 2017, 677 of which originated within DoD. The military departments reported 40 formal classification challenges. The "big six" IC agencies (CIA, DIA, NGA, NRO, NSA, and ODNI) reported a total of three formal classification challenges in FY 2017.

An 88% majority of the 721 formal classification challenges affirmed the original classification decision. In 8% of the challenges, however, the classification decision was overturned either in whole or in part, evidence that the classification challenge process uncovered inaccurate classification.

Outcomes:

Classification challenges serve a critical role by uncovering information improperly classified in the first instance and by providing a process for expedited declassification of information that no longer warrants classification. Classification challenges by authorized holders of classified information provides an internal check on the system by requiring a formal review and response from an impartial official or panel to determine the appropriateness of continued classification. Nearly all users of the security classification system agree that misclassification undermines the system to some degree. Incentives to use the formal classification challenge process, and training for authorized holders of classified information in how to use existing procedures, must support agency efforts to encourage more classification challenges.

FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW (FCGR)

Authority:

E.O. 13526, "Classified National Security Information," Section 1.9.

Findings:

In total, 21 agencies completed the FCGR in June 2017.

- 2,865 security classification guides (SCG) were reviewed.
- 221 SCGs were cancelled.
- 533 SCGs were consolidated.
- 14 new SCGs were written.

The total number of active SCGs at the end of the review was 2,154.

Agencies developed internal processes for reviewing SCGs, coordinating with Subject Matter Experts (SMEs), classification and declassification experts, users of the guides, and engaging with senior leadership to ensure compliance with criteria ISOO provided.

NGA completed an agency-wide consolidation effort of its guidance that was considered a best practice by ISOO for the FCGR. The Consolidated NGA (CoNGA) SCG merged all individual NGA SCGs into a single source containing validated and updated content for system users.

The final product achieved its primary goals of:

- Reducing the redundancy across NGA SCGs to meet DoD and ODNI requirements, as well as support ease of use by the NGA workforce,
- Improving the utility of classification guidance to enable efficient and effective Geospatial intelligence product development, and
- Modernizing the content of NGA's SCGs to reflect 21st century dynamic military operations.

To achieve these goals, the CoNGA SCG working groups developed and implemented the following:

- Enhancement statements labeled "Value," "Damage," and "Unclassified." The "Value" statement explains why the information is being protected. The "Damage" statement describes the potential impact to national security should an unauthorized disclosure occur. The "Unclassified" statement outlines how a user can address the classified line item in an unclassified manner.
- OCA reorganization. Each OCA is responsible for specific line items in the new guide allowing for more responsive modifications to the guide.

- Source/Method/Mission categories. Each category allows the OCA to further define why a line item is classified.
- Rapid change process. This new organizational process provides users an expedited means to request line item changes and/or clarifications.
- Security Management Resource Tool. The tool is a SharePoint product that enables users to search all line items in one central location.

Analysis:

Both the FY 2012 and FY 2017 FCGRs demonstrated agencies' efforts to streamline their classification guidance and more clearly identify categories of what information requires protection and safeguarding through security classification. The FCGR resulted in more uniform and consistent guidance, largely brought about by efforts to team SMEs with classification and declassification experts, program managers and technologists, who were more actively engaged in the FY 2017 FCGR than during the FY 2012 FCGR.

Agency use of security classification working groups and their ability to develop baseline and formalized criteria for the review of original classification decisions and SCGs supported this more extensive review. Agencies broadened the scope of their review to include the examination of policies, classification authorities, and training. Many agencies also made a concerted effort to determine whether the dissemination and availability of guidance was appropriate, timely, and effective.

ISOO determined the development of the CoNGA SCG to be a best practice because of its comprehensive approach to reviewing classification categories and its use of technology to assist users in making more accurate classification decisions. Senior agency leadership support for the CoNGA SCG directly impacted its development, adoption, and implementation successes.

Outcomes:

The FCGR remains an important investment in combating over-classification and limiting secrecy to only that information truly necessary to protect the national security. Future FCGRs should require extensive challenges to classification, emphasizing those goals achieved by the CoNGA SCG effort. Accurate and streamlined guidance will be required for a modernized security classification system that functions effectively and efficiently in the digital age.

Developing methodologies for standardizing SCG formats—particularly within the DoD and the IC—will ready SCGs for more integrated use in the electronic environment. Strong consideration should be given to developing single-topic SCGs that specific communities of interest would use. Shared equities will only continue to increase. Reducing the number of agency-specific guides will provide more consistent classification decisions across the executive branch. Providing appropriate levels of detail and formatting SCGs for machine readability will further support shared IT environments and common-use practices between agencies.

DECLASSIFICATION

AUTOMATIC, SYSTEMATIC, AND DISCRETIONARY REVIEW

Authority:

E.O. 13526, "Classified National Security Information," Sections 3.1, 3.3, 3.4.

Findings:

- Programmatic Declassification Activity Totals:
  - Pages Reviewed: 83,765,475.
  - Pages Declassified: 46,041,434.
  - Percent Declassified: 55%.
- Automatic declassification removes the classification of information at the close of every calendar year when that information reaches an age threshold of 25 years.
  - Pages Reviewed: 83,014,284.
  - Pages Declassified: 45,776,310.
  - Percent Declassified: 55%.
- Systematic declassification review is required for those records exempted from automatic declassification. Systematic declassification review occurs no later than 25 years after the original exemption from automatic declassification, dating the records at 50 years of age.
  - Pages Reviewed: 693,652.
  - Pages Declassified: 243,248.
  - Percent Declassified: 35%.
- 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.
  - Pages Reviewed: 57,539.
  - Pages Declassified: 21,876.
  - Percent Declassified: 38%.

Analysis:

The total page count for declassification review decreased by 18% under automatic, systematic, and discretionary declassification programs, the most significant under systematic declassification (87%). The rate of systematic declassification alone decreased significantly, from 79% to 35%, a reduction that applies only to records as old as

50 years or more. Although rates have nominally increased for automatic and discretionary declassification, the results of these processes remain unacceptably low at 55% for automatic declassification and 38% for discretionary declassification.

Still resource-intensive and paper-based, the declassification processes in place cannot meet the demands imposed by large volumes of paper records needing timely review, let alone the deluge of electronic records already well underway. At present, agencies can only parcel out limited resources to maintain declassification programs. They cannot adequately fund the development and adoption of available technologies that would improve workflow processes and support agile decision-making by declassification reviewers.

Under automatic declassification, the age of records determines how documents are selected for review. The current low declassification rate of pass-fail reviews under automatic declassification ensures a growing volume of records awaiting re-review. There is no method in place to provide an accurate estimate of how many records exempt from automatic declassification at 25 years currently await re-review at 50 years of age.

Since ISOO declassification assessments gave agencies relatively high program scores, the low declassification rates likely resulted from the correct application of overly risk-averse declassification guidance (see "Declassification Assessments"). Agency reviewers correctly applied restrictive guidance that errs on the side of continued declassification, reinforcing a risk-averse culture. Practices that interpret E.O. 13526 in ways that continue to produce excessively low declassification rates ignore the significant costs of securing classified records beyond 25 years, as well as the expense of re-reviewing records at 50 years of age.

Outcomes:

Challenges in declassification stemming from policy interpretation, implementation, and resource allocation will continue to persist without wide-ranging reforms to the underlying framework supporting declassification review. In particular, automatic declassification requires a major overhaul, beginning with the prioritization of records in response to public interest and an understanding of the historical value that federal records hold for research communities outside of the Government.

Agencies must revise policies that limit the scope of records exempted from automatic declassification under E.O. 13526. Agencies must work with the public to prioritize records for review under the constraints of limited resources. The backlogs generated by pass-fail review and excessively low declassification rates cannot be sustained. Ideally where technology and resources allow, agencies should strive to practice redaction review in lieu of pass-fail review methods.

Agencies need to redirect resources for the adoption of technological solutions that provide workflow tools and support decision-making during review. Current processes that demand multiple, line-by-line reviews by human declassifiers are unsustainable given the volume of records subject to automatic declassification.

Demonstrated technological solutions currently exist and must be implemented across agencies and the National Declassification Center (NDC) to ensure long-term success of these declassification programs. Existing and emerging technologies will improve risk management in declassification. Better risk management and less risk averse

agency cultures will lead to more accurate and timely review decisions that maximize information sharing and prevent the release of information that truly requires ongoing protection in defense of national security.

Costs will continue to drive declassification, influencing the volume and method of declassification review occurring (i.e. pass-fail or redaction method). Agencies will be better served to invest in technologies that assist declassification than to continue to fund outdated, paper-based processes that are unable to manage the review of classified electronic records.

MANDATORY DECLASSIFICATION REVIEW (MDR)

Authority:

E.O. 13526, "Classified National Security Information," Section 3.5.

Findings:

- MDR Requests:
  - Received: 6,540.
  - Closed: 4,581.
    - Estimated Declassified in Full: 51%.
    - Estimated Declassified in Part: 40%.
    - Estimated Denied Declassification: 9%.
  - Unresolved for over one year (backlog of requests): 20,556 (50% increase from FY 2016 reporting).
  - Number of agencies with requests unresolved for over one year: 11.
  - Number of referred requests received: 2,236.
- MDR Appeals:
  - Received: 635.
  - Closed: 359.
    - Estimated Declassified in Full: 28%.
    - Estimated Declassified in Part: 55%.
    - Estimated Denied Declassification: 17%.
  - Unresolved for over one year (backlog of appeals): 619.
  - Number of agencies with appeals unresolved for over one year: 9.
  - Number of referred appeals received: 446.

- Estimated Declassification Disposition Rates for FY 1996-2017 (Average):
  - Requests.
    - Estimated Declassified in Full: 64%.
    - Estimated Declassified in Part: 27%.
    - Estimated Denied Declassification: 9%.
  - Appeals.
    - Estimated Declassified in Full: 38%.
    - Estimated Declassified in Part: 37%.
    - Estimated Denied Declassification: 25%.

Analysis:

Each year, agencies struggle to close MDR requests and appeals, resulting in growing backlogs in need of processing. MDR programs were unable to keep pace with the thousands of requests and hundreds of appeals received. This trend is visible in the data for MDR requests over the last ten-year period, and appeals received over the last five years also clearly demonstrate this trend.

The number of requests and appeals unresolved for over one year continued to increase, with a significant spike in unresolved requests received in FY 2017 soaring to a high of 20,556 - a 50% increase from FY 2016. Almost all of those requests that remain unresolved for over one year were made at the National Archives and Records Administration (NARA), which include the Presidential Libraries. Requests taking longer than one year to process is a result of virtually all MDR requests requiring external consultation with one or more agencies. While referred requests continued decreasing for initial MDR requests, referred requests for appeals are increasing. This is likely the byproduct of more complex cases reaching the appellate level.

In FY 2017, ISOO is not reporting on the disposition of pages processed for MDR requests or appeals. ISOO identified issues with data reported by agencies that compromised our ability to accurately depict page count totals for requests and appeals declassified in full, declassified in part, or denied declassification. In reporting to ISOO, agency measurements were a mix of page numbers and document counts, making it impossible to provide an accurate page count of disposition totals for requests and appeals. As a result, for FY 2017, ISOO is not reporting on the disposition of pages processed for MDR requests or appeals. However, the data collected by ISOO offer a view of the percentage of use of the three dispositions when considering the total collection of records processed through the MDR program.

Analyzing MDR requests with the above considerations in mind revealed disposition for FY 2017 as follows: 51% of requests were declassified in full, 40% were declassified in part, and 9% were denied declassification. Earlier trends concerning disposition of MDR requests (since data collection began in FY 1996) were broken down as follows: 64% of requests were declassified in full, 27% were declassified in part, and 9% were denied declassification.

Although a mix of page numbers and document counts, the trends in the ratios of dispositions for MDR requests demonstrated significantly higher declassification rates than produced under automatic, systematic, and discretionary declassification programs. The same ratios were evident in the percentages for dispositions of appeals. This can be attributed to the more precise declassification decisions made through redaction review. The percentages are not as high for either the "declassified in full" or "declassified in part," likely due to the complexity of the records being appealed. Combined, however, these two declassification dispositions offered significantly higher declassification rates than produced under automatic, systematic, and discretionary declassification programs.

MDR appeals decided upon by the ISCAP similarly demonstrate higher declassification rates in MDR cases, which supports this analysis.

Outcomes:

Agencies having requests and appeals that remain unresolved for over one year will continue to struggle to satisfy the volume of requests made of their MDR programs. Similar to other declassification review programs, MDR programs require modernization to ensure their long-term viability. In particular, an increasing number of MDR requests result in unmanageable backlogs that plague NARA Presidential Libraries and DoD Joint Staff.

A recent strategic decision by NARA to centralize and relocate declassification review activity from the Presidential Libraries satellite locations to the Washington, DC area directly addresses the resource constraints on the overtaxed MDR system. Centralizing declassification review of Presidential records will streamline the referral process and reduce costs associated with transporting records until an interconnected technology framework is in place for broader declassification system.

Data collection and reporting guidance for agencies—particularly concerning the MDR program—require serious reform and modernization. Analysis of the reported FY 2017 declassification data revealed serious flaws in reporting, which likely were present in previous annual reports. The MDR program urgently requires a thorough modernization of the agency reporting process that must include the refining and updating of both the scope and subject matter of data taskings submitted to all executive branch agencies.

REVIEWS

DECLASSIFICATION ASSESSMENTS

Authority:

E.O. 13526, "Classified National Security Information," Section 5.2 (b)(4).

Findings:

Assessment results for agency 25-year declassification programs in FY 2017:

- National Aeronautics and Space Administration—High Score.
- Department of Justice—High Score.
- FBI—High Score.

Completion of two pilot assessments in FY 2017:

- Defense Information Systems Agency (DISA).
- NDC at NARA.

Analysis:

ISOO used information gathered in the pilot assessment at the NDC to refine and expand its oversight of agency application of 50-year exemptions granted to them by the ISCAP, while continuing to monitor agency 25-year programs. In particular, ISOO partnered with DISA to improve its declassification processes, focusing on the application of appropriate exemption authorities, the referrals of records, and the full and appropriate use of the Standard Form (SF) 715, "Declassification Review Tab."

Declassification assessment scores reflected appropriate application of agency declassification guidance during review. The results did not assess the appropriateness of the declassification instructions provided in the guidance.

Outcomes:

The declassification assessment program continues to support the strategic goal of improving the quality of agency declassification review programs. Since ISOO began the program in FY 2008, declassification assessment results demonstrate increased proficiency by agencies in three areas of major concern to declassification review: missed equities, improper exemptions, and improper referrals.

ISOO will continue its declassification assessment program in order to elevate the performance of declassification reviews across agencies, and to continue promoting best practices for accurate implementation of the requirements of E.O. 13526. Additionally, declassification assessments will begin to more fully scrutinize the appropriateness of declassification instructions provided in guidance, particularly concerning the review of records at 50 years of

age. ISOO will target at-risk declassification programs with on-site assessments, while exploring methodologies to decentralize and support agency self-inspections of program activities. Assessment outcomes will inform training efforts to assist in the improvement of declassification programs across Government.

SELF-INSPECTIONS

Authority:

Executive Order 13526, "Classified National Security Information," Section 5.2 (b)(2), 5.2 (b)(4), and 5.4 (d)(4).

Findings:

ISOO received 73 agency self-inspection reports in FY 2017, which included reports from individual DoD components.

- The data below utilize DoD information in the aggregate; so, the percentages are based on 46 agencies.

Self-inspection reporting yielded the following findings:

Document reviews conducted by agencies indicate discrepancies in the thoroughness, sample size, and scrutiny of document collections.

- Only 76% of agencies that classify information reported conducting document reviews, a fundamental requirement of self-inspection reporting.
    - ISOO document reviews found 1,129 discrepancies within 1,006 documents—a rate of 112.23 errors per 100 documents.
    - Agency document reviews found 80,852 discrepancies within 120,420 documents—a rate of 67.14 errors per 100 documents.
- **Core CNSI Program Requirements-**

Although full compliance with training derived from E.O. 13526 is required, we also consider and report if agencies come close to meeting this requirement:

- Initial Training- 91% of agencies reported that all of their cleared personnel received this training (identical to FY 2016 reporting).
    - 100% of agencies report at least 90% compliance (96% reported at least 90% in FY 2016 reporting).
- Refresher Training- 57% of agencies reported that 100% of their cleared personnel received this training (an increase from 52% in FY 2016 reporting).
    - 78% of agencies reported at least 90% compliance (identical to FY 2016 reporting).

- OCA Training- 68% of agencies reported that 100% of their OCAs received this training (identical to FY 2016 reporting).
    - The remainder of agencies (32%) reported less than 90% compliance (an increase from 23% in FY 2016 reporting).
- Derivative Classifier Training- 77% of agencies reported that 100% of their derivative classifiers received this training (a slight decrease from 78% in FY 2016 reporting).
    - 88% of agencies reported at least 90% compliance (identical to FY 2016 reporting).
- Performance Element- 41% of agencies report that 100% of the required personnel have this element (an increase from 39% in FY 2016 reporting).
    - 48% of agencies reported at least 90% compliance (an increase 44% in FY 2016 reporting)..
- **OCA Delegations and Classification Challenge Procedures**-
- OCA Delegations- 95% of agencies with OCA reported delegations are limited as required (a slight increase from 94% in FY 2016 reporting).
- Classification Challenge Procedures- 76% of agencies reported they have established classification challenge procedures (identical to FY 2016 reporting).
- **Marking Requirements**-
- Identification of Derivative Classifiers- Agencies reported reviewing a total of 105,892 documents to evaluate the application of this requirement (an increase from 89,250 in FY 2016 reporting).
    - Agencies reported 74% of the documents meet this requirement (a decrease from 77% in FY 2016 reporting).
- Listing of Multiple Sources- Agencies reported reviewing a total of 91,742 documents to evaluate the application of this requirement (an increase from 82,882 in FY 2016 reporting).
    - Agencies reported 71% of the documents meet this requirement (a slight decrease from 71% in FY 2016 reporting).
- **Agency Corrective Actions**-
    - 24% of agencies did not outline any corrective actions.
    - 20% of agencies only partially outlined any corrective actions.

Analysis:

Self-inspection reporting showed varying degrees of compliance and performance among agencies. Of concern, however, are the many agencies that reported an unacceptably low level of compliance with core CNSI program requirements, including training, performance evaluations, establishing classification challenge procedures, and applying marking requirements.

Of particular concern is the high error rate in document marking, found in both the self-inspections and the ISOO sampling. ISOO's finding of a much higher error rate on document reviews (66% greater) indicated a serious inconsistency in how ISOO and agencies conduct these reviews. While some of the error rate inconsistency may be due to scope and sampling differences, e.g. ISOO's sampling is of only 10 agencies, the preponderance of which were known or suspected of having weak document marking practices, this difference requires further examination to fully determine the cause, though even the rate of 67 errors per 100 documents found in agency self-reporting is itself unacceptably high.

Although most agencies reported conducting document reviews, ISOO document reviews found that there has been no improvement in marking of documents in the executive branch. In FY 2009, ISOO's document review assessment evaluated the performance of 15 agencies in a sampling of 1,565 documents. It found 1,805 discrepancies—a rate of over 115 errors per 100 documents, nearly the same rate ISOO found in FY 2017. The complexity of classification marking requirements contributed to these marking errors, as did a lack of effective training for derivative classifiers.

Over 24% of agencies did not outline any corrective actions after reporting deficiencies, and an additional 20% only partially outlined corrective actions. In total, 44% of agencies did not report they are taking comprehensive steps to correct all identified program weaknesses and deficiencies.

Although a slight improvement from last year, the level of compliance with the performance element requirement remained unacceptably low, which is troubling. The significance of this finding was only compounded by agencies reporting their inaction in taking corrective measures to address this program shortcoming, along with many others.

Outcomes:

The consistent underperformance of many agencies in multiple self-reported program elements clearly demands strategic change in the fundamental design and implementation of the self-inspection program, particularly as the role of information systems security continues to increase across programmatic functions. Trends are long and continuing—or in some areas worsening—and will require significant policy and technology changes to reverse.

Without increased resources, which ISOO does not anticipate, measuring the effectiveness and efficiency of the security classification system will depend on accurate and timely data reported by agencies through their self-inspection programs. Data collection methodology and reporting requirements need modernization to improve the efficiency and value of data submission, collection, and analysis. Efforts will focus on reducing redundancies, limiting the scope of reporting, and maximizing value for the overall system.

Agencies must examine their document review processes and their self-inspection programs in general to determine how to make them more effective in identifying and correcting classification and marking discrepancies. It is essential that knowledgeable personnel conduct the document reviews. Reviews must evaluate the classification and all required markings on a sufficient number of classified documents to make a credible assessment of their classification actions. Those agencies (24%) that classify information but reported no document review, must immediately begin conducting reviews of representative samples of their original and derivative classified actions.

ISOO will increase its outreach efforts to improve the CNSI self-inspection program. It will engage agencies having stronger self-inspection programs to provide information exchanges on methodologies, document review process-

es, tracking, and reporting, such as those provided at ISOO Open House events and training forums. It will continue researching more targeted and tactical data collection methodology. Focusing self-inspection reporting on a limited number of program elements will inform the efforts of agency training programs and will integrate program functions in support of a common improvement goal.

CNSI PROGRAM ON-SITE REVIEWS

Authority:

Executive Order 13526, "Classified National Security Information," Section 5.2 (b)(2) and (b)(4).

Findings:

On-Site Reviews- ISOO conducted full on-site reviews of four agencies' CNSI programs.

Agencies that received full reviews had deficiencies in multiple program elements.

- **Classification Guides**-
  - Two of four agencies had not reviewed their guides in over five years.
  - The classification guides at two agencies lacked some information required by 32 CFR 2001.15(b).
  - Of particular concern were guides at two agencies that prescribed the unauthorized use of a "25X" exemption as a classification instruction.
    - The agencies had not been granted authority by ISCAP to apply exemptions on newly created documents.
- **Security Education and Training**-
  - At three of the agencies, one or more of these training elements failed to address the minimum training requirements outlined in 32 CFR Part 2001.71.
  - At two agencies, interviews with derivative classifiers revealed a lack of understanding of basic classification principles.
- **Self-Inspections**- At one agency, the sample of documents reviewed was too small for the agency to make a credible assessment of its classified products.
- **Performance Appraisals**- At one agency, this rating element was not included in performance plans. A second agency's performance plan covered only the management of classified information, not its designation.
- **Safeguarding**-
  - At one agency the SF 701, "Security Activity Checklist," was not in use, with the effect that the end of the duty day produced no certification that work areas were properly safeguarded.

- At the same agency, there were offices in which it was unclear which equipment was used to process classified information and which was used to process unclassified information because the classification labels SF 706 through 710 were not being used.

ISOO conducted follow-up reviews of six agencies' CNSI programs.

- During six follow-up reviews, agencies addressed 39% of previous ISOO findings.
  - Three agencies addressed between 60% and 70% of ISOO findings.
  - Three agencies addressed between 15% and 33% of ISOO findings.
- **Information Systems Security Review-**

ISOO conducted full on-site reviews at four agencies' CNSI programs for information systems security compliance.

- Three agencies did not meet the requirement to have Plan of Actions and Milestones (POA&M) reviewed and updated within the last two years.
  - The POA&M is one of the key documents for assessing and authorizing classified information systems. The information contained in the POA&M is used by the authorizing official to monitor classified information systems' residual risk and vulnerabilities.
- Two agencies did not complete implementation of two-factor authentication on the Secret fabric.
  - The goal of this implementation was to strengthen verification of the identity of individuals logging on to classified information systems.

ISOO conducted follow-up reviews at five agencies' CNSI programs for information systems security.

- Follow-up reviews demonstrated agencies addressed 67% of the findings related to information systems security from the original full on-site review.
  - The most frequently occurring finding during the follow-up reviews was the absence of consistency in the assessment and authorization process.
  - The next most common finding was the lack of policy implementation and enforcement.
  - The third most common finding was the absence of a standard baseline for the configuration and deployment of Classification Management Tools by service providers.
- **Marking of Classified Documents-**
- Document Review Totals:
  - Number of Agencies Reviewed: 10.
  - Total number of documents reviewed: 1,006.
  - Number of documents with discrepancies: 641.

- Percentage of documents with discrepancies: 64%.
- Total number of discrepancies: 1,129.
- Average number of discrepancies per 100 documents: 112.
- Average number of discrepancies per document in the documents that contained discrepancies: 1.76.

- Frequently Occurring Document Discrepancies:
  - "Classified By" Line: 237 (24%).
  - Multiple Sources: 231 (23%).
  - Portion Marking: 208 (21%).
    - 79 were major, as they lacked all or nearly all of the required portion markings.
    - 129 were minor, as most of the document was properly portion marked but one or several portion markings were missing.
  - Declassification: 132 (13%).
  - "Derived From" Line: 96 (10%).
  - Date of Origin: 49 (5%).
  - "Reason" Line: 48 (5%).
  - Marking: 48 (5%).
  - Over-classification: 40 (4%).
- Eight of the 10 agencies had marking error rates ranging from 59% to 78%.
- Two agencies had fewer errors, 20% and 35%.

Analysis:

The results of the on-site review program demonstrated a lack of agency compliance with core requirements of E.O. 13526. Follow-up reviews showed agencies did not address ISOO findings from the initial reviews. Although agencies had at least two years to make improvements, no agency addressed all the findings identified in the initial review, and half of the agencies addressed only 30% or fewer. Ironically, those agencies with the greatest need for improvement in their CNSI programs did not address the findings. The failure to address the findings of ISOO reviews strongly suggested a lack of agency senior leadership commitment to ensure adequate implementation of their CNSI programs. It also indicated ISOO's assessments and findings were likely too broadly scoped for agencies to understand and address. As such, review programs were not able to accomplish the goals of consistent agency improvement in core CNSI program elements.

Reviews of classified information systems found that the most significant areas at risk center on the processes and methodology used by agencies when assessing and authorizing those systems. Appropriate internal assessment and authorization processes are foundational to providing an effective information systems security program across agencies.

Likewise, the proper marking of classified information is essential to the integrity of the security classification system. Agencies with fewer marking errors implemented marking tools and templates, had quality control processes, and managed more effective self-inspection programs that reviewed samples of classified documents on a consistent basis.

Even when marking errors are minor, and thus do not necessarily risk immediate damage to national security, these errors still have severe consequences. Information sharing and timely declassification are at risk when managing improperly marked documents. A 63% error rate in the marking of classified documents is unacceptable. This is particularly concerning considering the ample amount of security education and training available. The strength and effectiveness of agency security education and training came into serious question given the error rate found in document marking. Education and training efforts, particularly for derivative classifiers, did not achieve their desired outcomes.

Outcomes:

For the future of on-site reviews, rather than assessing programs holistically at each agency—and thus only having resources to address a very few each year—assessments and findings on program improvement will be more focused and tactical in nature. Revamping the on-site review process and coupling it more closely with agency self-inspection practices will foster an oversight strategy more in line with a continuous monitoring approach. The ISOO review process will focus on improving compliance with individual CNSI program elements across a broad range of agencies. The agencies, in turn, will be required to sustain these improvements over time through their self-inspection programs, with ISOO providing oversight.

Agencies must address and correct ISOO on-site review findings, particularly in the areas of information systems security and the marking of classified information. ISOO will require periodic updates until all findings have been addressed and closed. Both the on-site review program and self-inspection program must significantly influence the priorities of agency resource allocation for their CNSI programs. Information systems security will become an increasingly essential program element as its role in the CNSI program will only continue to expand in scope and size across agencies.

As noted with the self-inspection program, there has been a long and continuing trend in agency underperformance in the proper application of classification and marking requirements, as well as inconsistencies in the implementation of requirements for other essential CNSI program elements. Changes to the on-site review process will be necessary to improve agency compliance. Reforming education and training efforts must complement these changes.

In addition, policy and technology reforms will be needed to simplify and reduce the effects that analog processes have on classification and declassification. Automation and technological intervention to support decision-making will be critical to CNSI program improvement, as will an interconnected oversight program able to function effectively in a limited resource environment.

INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL (ISCAP)

Authority:

E.O. 13526, "Classified National Security Information," Section 5.3.

Findings:

The ISCAP reported the following data for FY 2017:

- Appeals received: 577 (80% increase).
- Appeals decided upon: 50.
- Documents decided upon: 338.
  - Documents declassified in full: 197 (58%).
  - Documents declassified in part: 119 (35%).
  - Documents affirmed: 22 (7%).
- Declassification guides received: 23.
- Number of public meetings: 1.
- Classification Challenge Appeals: 0.

Analysis:

The declassification decisions rendered by the ISCAP continued to demonstrate the effectiveness of an interagency declassification process in achieving more accurate release of records. Appeal decisions by the ISCAP resulted in an increase in declassified information in 93% of the appealed documents decided upon in FY 2017. Since its establishment in 1996, the ISCAP has decided upon 2,935 documents, averaging an over 75% declassification rate in its decisions.

The number of MDR requests appealed to the ISCAP continues to increase each year. Overall, the increase in the number of appeals to the ISCAP may be in part due to its proven higher declassification rate in appeal decisions. The dramatic increase in requests to the ISCAP in FY 2017, however, resulted from a single appellant, whose 450 appeals comprised 78% of all appeals received. Despite the impact of a single appellant on the FY 2017 data, the number of appeals received in the previous five years and the page counts in those appeals both illustrated the growing workload for the ISCAP, which has contributed significantly to a rising backlog of appeals awaiting decision.

As part of the MDR appeal process, the ISCAP receives appeals due to agencies not providing a final decision on an MDR request within the allotted one-year timeframe, which also significantly impacted the growing backlog of

appeals awaiting decision. The portion of appeals reaching the ISCAP because of the missed one-year timeframe was 76% in FY 2017, compared to 71% in FY 2016, 24% in FY 2015 and 18% in FY 2014.

The ISCAP devoted a considerable amount of its resources to the review of declassification guides submitted by 23 agencies in FY 2017. It will conclude the review in FY 2018. Lessons learned from the 2012 review assisted the ISCAP in re-evaluating agency authorities for the exemption of information at the 25, 50, and 75-year milestones.

Outcomes:

The ISCAP must return to its "sole purpose of advising and assisting the President." The backlog of appeals will continue to significantly impact the work priorities and resources of the ISCAP without intervention. The ISCAP bylaws allow the ISCAP staff discretion in prioritizing appeals for decision. Considerations include the age, size, complexity, and type of the appeal, as well as the type of appellant and relevant declassification breakthroughs that may impact decisions. Still, changes to the bylaws and E.O. 13526 are needed to refocus the appeals workload on high-value records of public interest, as was the original intent of the ISCAP appeals process. ISOO will continue its collaboration with the NSC to propose revisions to E.O. 13526 to address these and other concerns in need of modernization.

The growing backlog results from a handful of appellants seeking access to records specific to their research interests. Current policies and procedures permit the commitment of a gross amount of very limited resources to the appeals of these relatively few, serial appellants, regardless of the value of, or public interest in, the information requested.

Amending the bylaws and E.O. 13526 by reforming automatic declassification, adjusting MDR deadlines, and reexamining declassification guide reviews will decrease the amount of records appealed to the ISCAP. The ISCAP should recommend expanding its membership to include a member of the public (able to obtain the appropriate security clearances) and to agencies with expanded and growing CNSI programs, such as DHS. The role of the public citizen would be to garner support for any improvements the ISCAP adopts and would enhance sustained credibility in ISCAP decision-making activities.

On June 1, 2017 the ISCAP held its first appellants forum to share information about the growing numbers of appeals and the increasing backlog in the ISCAP workload. Nearly 100 appellants, agency declassification staff, and civil society observers of the security classification system participated and shared their views with the ISCAP staff and membership.

The interaction between the ISCAP staff and its stakeholders increased awareness by appellants of the impact multiple appeals from singular appellants has on the ISCAP process and its ability to render decisions. The ISCAP staff saw concerted efforts by some appellants to streamline and prioritize their appeals. The ISCAP will hold another forum in the summer of 2018, continuing to engage with its stakeholders in order to process appeals as efficiently and effectively as its resources will allow.

The ISCAP staff will also continue to explore and pilot the use of IT workflow tools to assist in ISCAP business processes. It will provide information about ISCAP appeal decisions on its website to inform agency declassification programs of precedent-setting declassification actions that should inform agency declassification guidance. Oversight and training programs will continue to monitor and assist in the proliferation of ISCAP decisions to increase the timeliness and accuracy of agency guidance for the improvement of declassification programs across Government.

COST ESTIMATES FOR SECURITY CLASSIFICATION ACTIVITIES

Authority:

E.O. 13526, "Classified National Security Information," Section 5.4 (d)(8).

Findings:

Government:

- Government security classification cost estimates totaled $18.39 billion, an increase of 9% from FY 2016 reporting.
  - Personnel Security: $2.14 billion (10% decrease).
  - Physical Security: $2.63 billion (8% increase).
  - Classification Management: $387.53 million (1% increase).
  - Declassification: $102.58 million (5% decrease).
  - Protection and Maintenance for Classified Information Systems: $6.59 billion (4% increase).
  - Operations Security and Technical Surveillance Countermeasures: $237.81 million (13% increase).
  - Professional Education, Training, and Awareness: $835.64 million (14% increase).
  - Security Management, Oversight, and Planning: $5.45 billion (28% increase).
  - Unique Items: $26.5 million (30% increase).

Industry:

- DSS provided a total security classification cost estimate for industry of $1.49 billion, an increase of almost 17% from FY 2016 reporting.

Analysis:

Security classification costs continued to increase across almost all categories of cost estimate reporting. Personnel security; physical security; protection and maintenance for classified systems; and security management, oversight, and planning remained the categories of greatest expense for Government, totaling in the billions of dollars in each of the four functions. The percentage of Government spending on declassification continues to decrease every year. Decreased spending on declassification results in higher long-term costs associated with physical security and the protection and maintenance for classified systems. The increasing volume of records and data in need of declassification review will require large expenditures that potentially could be curtailed with increased declassification.

Agencies' methodologies for calculating cost estimates followed provided guidance, yet inconsistencies remained. In particular, agency feedback indicated difficulty in measuring the cost estimates for security classification in categories of overlapping security requirements, such as work force, facility, and information systems protection. The

hybrid information environment based on paper and digital records also posed an increasing challenge in reporting accurate and precise cost estimates for Government. Agencies incur fluctuations in costs for information security systems, in part because the purchase and upgrading of systems do not occur through a federated process on a consistent schedule due to the varied mission needs of agencies. These challenges led to difficulty in verifying reported cost estimates for the entire CNSI program.

Outcomes:

There is a serious need to modernize the cost estimate methodology and reporting process used across agencies to enhance the accuracy of the cost estimates provided to ISOO. The inability to audit or reconstruct agency data submissions is a concern that undermines the entire cost-estimate reporting process.

Until security classification costs are an expected line item in agency budget requests, both estimating costs and securing resources for security classification functions will remain significant challenges for agencies to complete, which greatly impacts planning and modernization efforts, particularly in the area of information systems security. IT modernization efforts, particularly those intended to be executive branch-wide, must better incorporate security classification functions into policy and implementation execution. The impact of security classification functions on agency missions and programs needs to be relayed more effectively to senior agency leadership and to OMB.

NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

Authority:

E.O. 12829, "National Industrial Security Program," 32 CFR Part 2004-National Industrial Security Program Directive No. 1.

Findings:

ISOO continued its work on a new Implementing Regulation as part of 32 CFR 2004 for the NISP, which is in final coordination at OMB.

- Policy discussions centered on NISP core elements including consistent oversight and eligibility standards across Cognizant Security Agencies (CSA), consistency with the NISP Operating Manual (NISPOM), and streamlined procedures for National Interest Determinations (NID).
    - In order for a company cleared under a Special Security Agreement (SSA) to have access to proscribed information, the Government must approve a NID that states release of proscribed information to the company is consistent with the national security interests of the United States.
- Updates included the addition of the DHS Classified Critical Infrastructure Protection Program (CCIP) and its role as a CSA.

Outreach efforts to NISP-based organizations include ISOO assistance at the American Society for Industrial Security International, Defense and Intelligence Council (D&IC), Industrial Security Awareness Councils, Aerospace Industries Association, National Defense Industrial Association, National Classification Management Society, and the National Security Institute.

NISP Policy Advisory Committee (NISPPAC) meetings were held on November 10, 2016 and May 10, 2017 and focused on a variety of program elements of the NISP.

- Security clearance investigation backlogs: The current clearance backlog continued to be excessive to the extent that it is affecting the ability of industry to meet classified contract requirements. Concerns by stakeholders included contract stoppage, inability to find properly cleared personnel, and a lack of sufficient resources to decrease the backlog.
- DSS in Transition: DSS was in the process of creating asset focused, threat-based reviews of industry. The concept is significantly different than the routine NISPOM compliance-based security vulnerability assessments of classified information at contractor-cleared locations. It encompasses both classified information and CUI.
- Transfer of Investigations: A large portion of the clearance investigation mission will be transferred to DoD and will be managed by DSS, to include NISP contractor clearances. Concerns include successful transfer of all investigations, lack of DSS resources to reduce the backlog, lack of continuity in the transfer, and additional delays due to the transfer process.
- Continuous Evaluation (CE): CE is a new method by which cleared individuals are continuously monitored

in addition to the periodic reinvestigation (PR). As opposed to the current static PRs, CE's goal is to identify and adjudicate derogatory on a real time basis, and unusual or out-of-the-norm behavior before or at the time in which it occurs. Concerns with this new process include proper implementation, methods of submission, integration with insider threat programs, and thresholds for clearance revocations.

- New Systems/Databases: There were four clearance related systems in development, some of which were in deployment phases and all of which required industry's involvement: the Defense Industrial System for Security, the National Industrial Security System, the NISP Contracts Classification System, and eApp. Primary concerns were lack of sufficient training, lack of resources to manage the systems, deployment of several systems in the same timeframe, and industry's need for inclusion on system progress and deployment dates.
- NISPPAC data for Federal Advisory Committee Act (FACA) Program: This review was completed to ensure compliance, with no significant findings reported and approval granted for the continuation of the NISPPAC.

The NISPPAC Working Groups (WG) addressed program elements in need of reform for the NISP.

- Clearance: The Clearance WG met prior to both NISPPAC meetings and general topics were the clearance backlog, current investigation timeline statistics, and the transfer of investigations to DoD.
- NISPOM Re-write: The NISPOM re-write was under internal review and coordination at the Office of the Under Secretary of Defense for Intelligence.
- Insider Threat: The Insider Threat WG completed its discussion on Phase 1 of the program. In Phase 1, DSS required contractors to name an Insider Threat Program Manager and to train all employees on the requirements of the program. It will not meet again until DSS has implemented Phase 2 of the program.
- NID: The NID WG discussed the delay on NID decisions and the process for NIDs by each CSA. Consensus was that there were many issues with the NID process and that further discussion was needed for resolution and to ensure reciprocity across the CSAs. The group will not meet again until the release of the 32 CFR 2004, which focuses on reciprocity and consistent procedures.

Analysis:

The NISP continued to support improving the partnership between Government and industry through the various activities of the NISPPAC. Security clearance investigation reform remained a focus area where high risk persists for Government and industry due in large part to the inability to share eligibility and access information across the various agency systems. The backlog of security clearance investigations negatively impacted industry contract performance and industry access to Government installations and military bases. The reforms to the NISPOM provided an opportunity to establish enhanced insider threat program across agencies and to apply consistent standards for all CSAs to determine contractor eligibility for access to classified information.

Outcomes:

ISOO will continue its oversight of the NISP, most noticeably through the efforts of the NISPPAC. The NISPPAC WGs will continue to prioritize primary focus areas in need of reform, particularly concerning information systems security as related to insider threat, CE practices, and information systems authorization. The impact of the implementation of the CUI program on the NISP remains unclear and will require increased industry collaboration and participation on ISOO efforts concerning CUI policy interpretation, training, and oversight.

CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM

CUI IMPLEMENTATION

Authority:

E.O. 13556, "Controlled Unclassified Information," and 32 CFR 2002, "Controlled Unclassified Information."

Findings:

ISOO, as the CUI Executive Agent, issued CUI Notice 2016-01, "Implementation Guidance for the Controlled Unclassified Information Program," on September 14, 2016.

The notice established phased implementation deadlines and directed that, for FY 2017:

- By May 14, 2017, agencies must have:
  - appointed CUI SAOs and program managers (if they had not yet done so in response to an April 2013 memorandum to agency heads),
  - developed and published the agency's CUI policy, and
  - assessed current information systems and developed plans for compliance as needed.
- Within 180 days thereafter, agencies must have:
  - developed and deployed CUI training to all affected agency employees, and
  - implemented or verified that all physical safeguarding requirements were in place.

ISOO developed the deadlines in conjunction with OMB.

All executive branch agencies were required to provide ISOO with status updates on May 31, 2017, and annual reports at the end of FY 2017. ISOO required that annual reports provide agency estimated costs incurred for CUI implementation in FY 2017.

Based upon information received from numerous agencies, ISOO determined that 136 agencies are responsible for implementing CUI programs. Additional agencies will be receiving CUI Program support or implementation from one of these responsible agencies.

- **Reporting–**

ISOO received the required annual reports from 61 of the 136 agencies (45%), including all but two of the cabinet-level departments, the Departments of Commerce and Energy.

- CUI SAOs and program managers-
  - 105 agencies reported appointing CUI SAOs and program managers.
- Policy-
  - Six agencies reported issuing CUI implementing policies.
  - 11 agencies reported having policies under internal review and near finalization.

- 30 agencies reported having policies in development and projected for issuance in FY 2018.
- 12 agencies reported policies projected for issuance in FY 2019.

- Costs and budget information-
  - Agencies did not receive funds for CUI implementation or programs in FY 2017.
    - The CUI regulation became effective during FY 2017 and OMB Circular A-11 for 2015 did not require agencies to submit CUI implementation budget requests for FY 2017.
    - As a result, agencies used existing personnel and resources for all CUI implementation activities during FY 2017.
  - Agencies expressed, formally and informally, serious concerns regarding the costs associated with implementation.
    - Some agencies reported a high likelihood of being unable to successfully and fully implement without additional funding earmarked for CUI implementation.
    - Some of the concerns were based on lack of funding and actual agency cost analysis.
    - However, some were not based on actual assessment of program implementation needs or costs; just sweeping assumptions and generalizations.
  - Some agencies provided itemized projections of implementation costs in FY 2017.
  - Some agencies informally reported that CUI implementation was not included in budget requests submitted to OMB in late FY 2017 and early FY 2018 despite requirements in the 2016 OMB Circular A-11, Part 2, section 31.15, and despite internal budget submissions from their CUI program offices.

- Information systems-
  - Six agencies reported having assessed and transitioned all information systems to meet CUI requirements.
  - A majority of agencies projected completing information system assessments in FY 2018 or FY 2019.
  - A number of agencies, particularly agencies that deal with comingled CNSI and CUI, expressed a need for a Government-wide technology strategy for marking, identifying, analyzing, contracting, and managing CUI. They also emphasized that it should integrate with systems for managing CNSI so agencies can reduce duplication and costs and better protect and share both kinds of information. Many agencies reported that the lack of such a technology strategy would adversely impact protection of both CNSI and CUI and implementation of the CUI Program.

- Physical safeguarding-
  - 36 agencies reported either planning (22), assessing (12), or modifying (2) physical environments to meet CUI requirements.

- CUI Registry-
  - The CUI EA added seven new categories in FY 2017 based on agency submissions.
  - Four existing categories were revised, updated, or given additional authorities.

- Three agencies continued to express the need for suitable authorities to address law enforcement gaps in the CUI Program, which ISOO and agencies previously identified in 2013.
  - Under the CUI Program, only law, regulation, or Government-wide policy can serve as the authority for protecting information.
  - The gap information cannot be treated as CUI unless an agency, group of agencies, or other entity with appropriate regulatory authority issues a regulation or Government-wide policy permitting or requiring its protection.
- Despite extensive discussions in previous years, ISOO facilitation efforts, and OMB approval, the agencies stalled on issuing a blanket authority to cover these gaps.
  - In FY 2017, ISOO initiated efforts to reignite cooperation to address these gaps; these efforts are ongoing.

- Training-
  - 26 agencies reported initiating or engaging in some form of CUI awareness training.
  - 24 agencies reported projected deployment of CUI training in FY 2018.
  - 16 agencies reported projected deployment of CUI training in FY 2019.

- **Federal Acquisition Regulation (FAR)–**
- General Services Administration (GSA) established a FAR team to develop a FAR case that will apply CUI requirements to Federal contractors.
- GSA projects the case will move to the Civil Agency Acquisition Council review stage in FY 2018.

Analysis:

The lack of finalized CUI agency policies was a major implementation gap that impeded the phase-out of the present Sensitive But Unclassified/For Official Use Only information regime. It also seriously hindered implementation of dependent core elements of the CUI Program, including training, assessment of information systems, physical security requirements, self-inspection programs, and agency component flow-down policies.

Assessing the cost of CUI Program implementation remained challenging. OMB's 2015 Circular A-11 did not direct agencies to include budget and cost estimates and requests for FY 2017. ISOO did request such information for the required report due at the end of FY 2017. Most agencies, however, either did not include any cost information or made only general statements that could not be verified. In contrast, some agencies reasonably articulated and assessed budget and cost estimates in their reporting.

Agency non-compliance with the requirement to appoint a CUI SAO and program manager responsible for CUI program adoption contributed to delays in policy finalization and implementation.

Agency status reports demonstrated the need for continuing oversight of agency CUI Program implementation efforts.

The aggressive phased implementation steps and deadlines were developed with agency input, ultimately refined and approved by OMB. They were developed on the basis of several underlying facts, which also underlie expectations about CUI Program implementation costs:

- Agencies were already protecting all of the information that falls within the scope of the CUI Program so would not have to begin anew.
- Agencies already had policies, physical safeguards, training, and information systems security processes and practices in place for this information that would need only moderate modifications to account for the CUI requirements.
- The majority of agency information systems were already operating at the CUI baseline standard of moderate confidentiality.

Although many agencies made progress on implementation, and some made significant progress, most agencies were not able to meet the requirements of the phased implementation schedule for a number of reasons. The varying size, complexity, and unique aspects of agency information regimes contributed to delays in adoption, as did a number of other impediments:

1. **Insufficient high-level support**. The CUI SAO and program manager were too low within some agencies, or located in an office that was not in a position appropriate to handle the program. In some agencies, the CUI Program was not deemed important enough to appoint a CUI SAO or program manager, or to include in budget submissions. CUI program offices have been established inconsistently across agency offices, including in records management, security, general counsel, CIO, and other offices. Some of these offices are not well-equipped to implement the CUI program because of a lack of understanding about information security and management or a lack of authority within the agency.

   Two cabinet-level agencies, the Departments of Commerce and Energy, have still not appointed CUI SAOs or program managers more than a year after implementation began across the executive branch. Many others did not respond to formal requests for status reports. Some agency heads had not informed their senior managers of the need to implement or to engage with the CUI program manager. Other agencies stated they were waiting to see whether the CUI Program would be canceled.

2. **Lack of funding.** There was a direct correlation between agency funding and agency implementation progress. OMB's 2015 Circular A-11 did not direct agencies to include budget and cost estimates and requests for FY 2017. Consequently, agencies made use of existing staff and resources, negatively affecting the pace of CUI implementation. Many staff were performing CUI functions as additional duties and thus simply did not have sufficient time to develop a comprehensive agency program. Without financial support, information systems assessments and planning were put off until another year.

   Many of the smaller agencies were able to carry out the first implementation phases despite lack of funding. These smaller agencies had far fewer offices or functions and fewer types of CUI to address. Many of the largest or most complex agencies, however, were not able to meet initial implementation phases and project-

ed another year or more to complete them. Some agencies were able to allocate funding to their CUI programs, including hiring contractors to assess systems or to assist with policy or training development. Others developed creative approaches to integrate their CUI system assessments into already-existing system review processes.

3. **High turn-over in agency CUI officials**. In many agencies, the CUI officials who worked for years on the CUI Program as it developed either retired or left. The CUI Program was often moved to a different office as a result. This significantly slowed implementation as the new officials were often entirely unfamiliar with the CUI Program and the agency's previous actions, agreements, and development. The learning curve was significant each time an agency's program changed ownership. In some cases, the new officials decided to undo all previous progress and agreements or to make significant changes to the course of the agency's implementation. In part, some of this turn-over was a ripple effect of the lack of high-level support and funding.

4. **Mistaken assumptions about the scope and nature of CUI and resistance to change**. Some agencies viewed the CUI Program as burdensome and too extensive to implement because they made unfounded assumptions about the CUI Program. For example, some were under the false assumption that the CUI Program creates new kinds of protected information or radically changes safeguarding or dissemination requirements. Other agencies underestimated the scope of information managed by their CUI Program. Some officials were resistant to change. ISOO's awareness and outreach efforts are working to reduce the number of these agencies.

5. **Limited planning and assessment up front.** Many agencies did not begin planning or preparing for implementation during the development years. Other agencies attempted implementation without a comprehensive plan or assessment of the types and amounts of CUI at their agency.

To combat these impediments, ISOO engaged with agencies individually to answer questions, provide briefings to various levels of management, and assist with specific implementation concerns. ISOO also issued implementation guidance and notices on common topics, and began conducting oversight reviews of completed agency policies and self-reported progress to provide the agencies with individual recommendations and feedback. Its implementation working group facilitated sharing of best practices and interagency successes to provide additional agency support.

ISOO provided agencies with a mechanism to remain in compliance when unable to meet the aggressive timelines of phased implementation. Many agencies took advantage of the mechanism by demonstrating reasonable progress, providing regular status reports, and offering projected completion dates based on unique agency challenges.

Outcomes:

Without White House intervention to emphasize the need for top-level agency support and funding, CUI Program implementation will be significantly delayed. This leaves appropriate information protection and sharing for unclassified controlled information in serious jeopardy.

Agencies must complete budget requests consistent with OMB Circular A-11 and submit cost estimates and projections as part of their CUI annual reports. Otherwise, ISOO will be unable to assess potential burdens and costs across the executive branch. ISOO's assessment will be critical to informing resource allocation for implementation and maintenance.

Agencies must move expeditiously to revise policies to achieve remaining implementation requirements. The lack of finalized CUI policies at agencies is in need of serious attention in FY 2018. Additionally, agencies must move forward to issue or revise joint Federal regulations or Government-wide policies to establish CUI categories where needed, or individual ones when the information is under their sole responsibility.

Without sufficient top-level support and commitment, implementation will continue to drag. Where not already done, agencies must appoint CUI SAOs and program managers to oversee the CUI Program in their agencies. Agencies must also examine the appropriateness of where CUI responsibility is located within the agency, and must try to reduce turn-over in CUI officials. Those CUI officials unable or unwilling to make changes necessary to adopt the CUI Program must be removed.

With White House and agency collaboration, the CUI EA must initiate a working group to explore developing a Government-wide technology strategy for managing CUI—to include identifying, marking, analyzing, contracting, quality-control, and other aspects. This will help combat improper safeguarding or sharing procedures, significantly reduce marking and managing burdens on agencies, increase standard practices, and allow for better integration with CNSI security requirements, especially for agencies that comingle classified and controlled information.

APPENDIX: REPORTED DATA

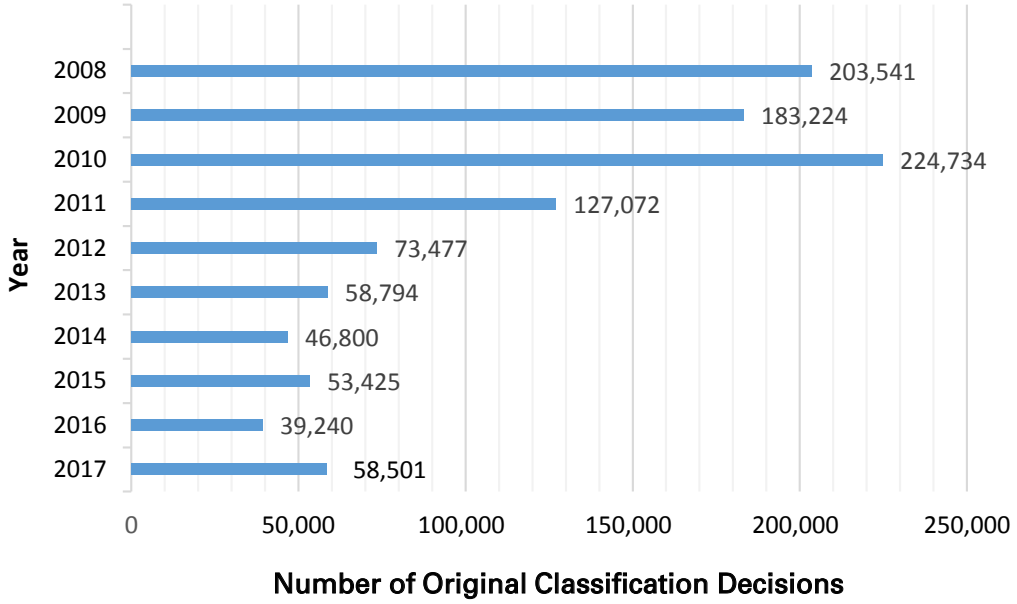
Original Classification Authorities

FY 1998–2017

Year	Original Classification Authorities						
	Number of TOP SECRET OCAs	Percentage of TOP SECRET OCAs	Number of SECRET OCAs	Percentage of SECRET OCAs	Number of CONFIDENTIAL OCAs	Percentage of CONFIDENTIAL OCAs	TOTAL Number of OCAs
1998	884	22.65%	2,773	71.05%	246	6.30%	3,903
1999	879	22.85%	2,707	70.38%	260	6.76%	3,846
2000	934	22.62%	2,981	72.18%	215	5.21%	4,130
2001	998	24.15%	2,945	71.27%	189	4.57%	4,132
2002	929	23.19%	2,898	72.34%	179	4.47%	4,006
2003	936	23.53%	2,921	73.43%	121	3.04%	3,978
2004	958	23.91%	2,911	72.65%	138	3.44%	4,007
2005	994	25.11%	2,864	72.34%	101	2.55%	3,959
2006	1,032	25.53%	2,912	72.04%	98	2.42%	4,042
2007	1,040	25.19%	2,980	72.19%	108	2.62%	4,128
2008	1,016	24.73%	2,968	72.23%	125	3.04%	4,109
2009	923	36.10%	1,530	59.84%	104	4.07%	2,557
2010	901	37.89%	1,463	61.52%	14	0.59%	2,378
2011	905	38.31%	1,441	61.01%	16	0.68%	2,362
2012	898	38.61%	1,415	60.83%	13	0.56%	2,326
2013	886	39.05%	1,371	60.42%	12	0.53%	2,269
2014	884	38.84%	1,381	60.68%	11	0.48%	2,276
2015	850	38.65%	1,336	60.75%	13	0.59%	2,199
2016	860	38.83%	1,325	59.82%	30	1.35%	2,215
2017	716	38.35%	1,114	59.67%	37	1.98%	1,867

Original Classification Activity

FY 2008–FY 2017



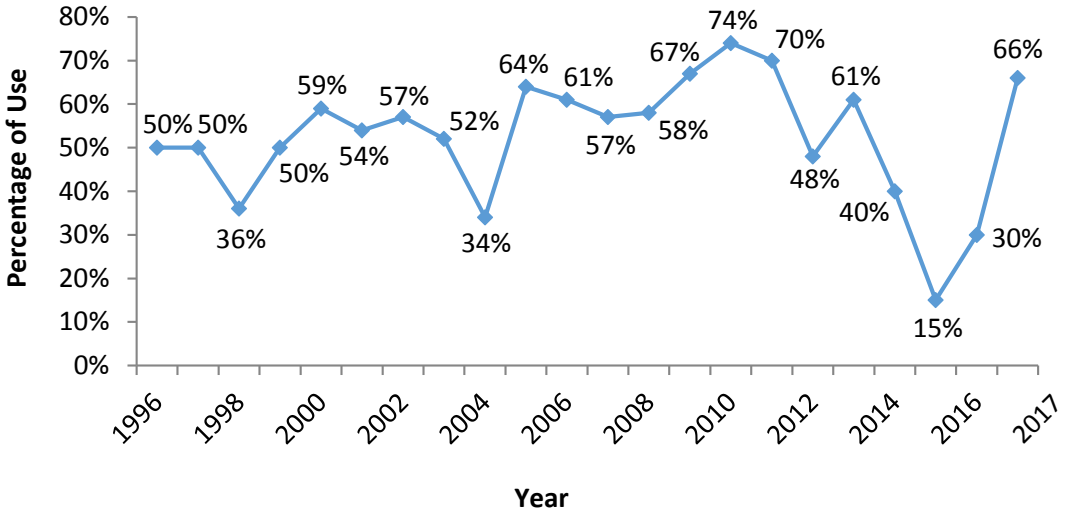
Original Classification Activity by Level of Classification

FY 1998–FY 2017

Year	Original Classification Decisions						
	Number of TOP SECRET Original Classification Decisions	Percentage of TOP SECRET Original Classification Decisions	Number of SECRET Original Classification Decisions	Percentage of SECRET Original Classification Decisions	Number of CONFIDENTIAL Original Classification Decisions	Percentage of CONFIDENTIAL Original Classification Decisions	TOTAL Number of Original Classification Decisions
1998	4,872	3.56%	91,516	66.80%	40,617	29.65%	137,005
1999	3,601	2.12%	125,903	74.18%	40,231	23.70%	169,735
2000	6,446	2.92%	106,494	48.17%	108,129	48.91%	221,069
2001	11,941	4.58%	155,144	59.52%	93,593	35.90%	260,678
2002	11,463	5.28%	114,237	52.57%	91,588	42.15%	217,288
2003	6,610	2.82%	142,594	60.92%	84,848	36.25%	234,052
2004	11,435	3.26%	258,762	73.69%	80,953	23.05%	351,150
2005	12,406	4.80%	183,504	70.95%	62,723	24.25%	258,633
2006	7,264	3.13%	174,204	75.09%	50,528	21.78%	231,996
2007	7,727	3.31%	180,714	77.35%	45,198	19.35%	233,639
2008	5,712	2.81%	163,727	80.44%	34,102	16.75%	203,541
2009	4,407	2.41%	140,236	76.54%	38,581	21.06%	183,224
2010	4,194	1.87%	181,045	80.56%	39,495	17.57%	224,734
2011	18,522	14.58%	68,624	54.00%	39,926	31.42%	127,072
2012	9,608	13.08%	39,557	53.84%	24,312	33.09%	73,477
2013	2,732	4.65%	39,384	66.99%	16,678	28.37%	58,794
2014	5,175	11.06%	31,200	66.67%	10,425	22.28%	46,800
2015	2,142	4.01%	36,151	67.67%	15,132	28.32%	53,425
2016	1,850	4.71%	27,113	69.10%	10,277	26.19%	39,240
2017	1,398	2.39%	48,056	82.15%	9,047	15.46%	58,501

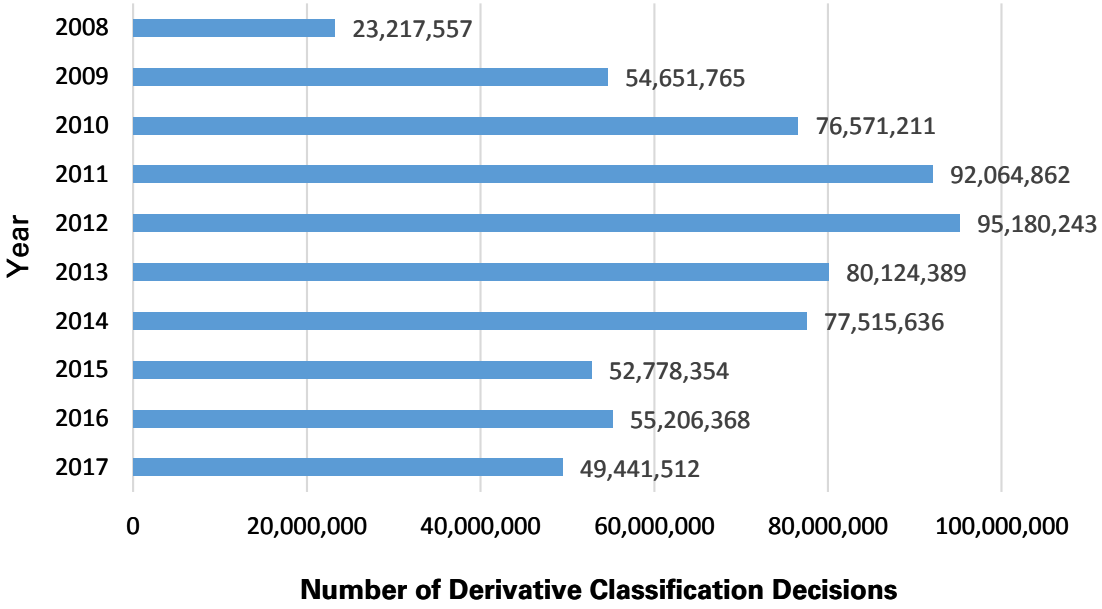
Use of the "Ten Years or Less" Declassification Category

FY 1996–FY 2017



Derivative Classification Activity

FY 2008–FY 2017



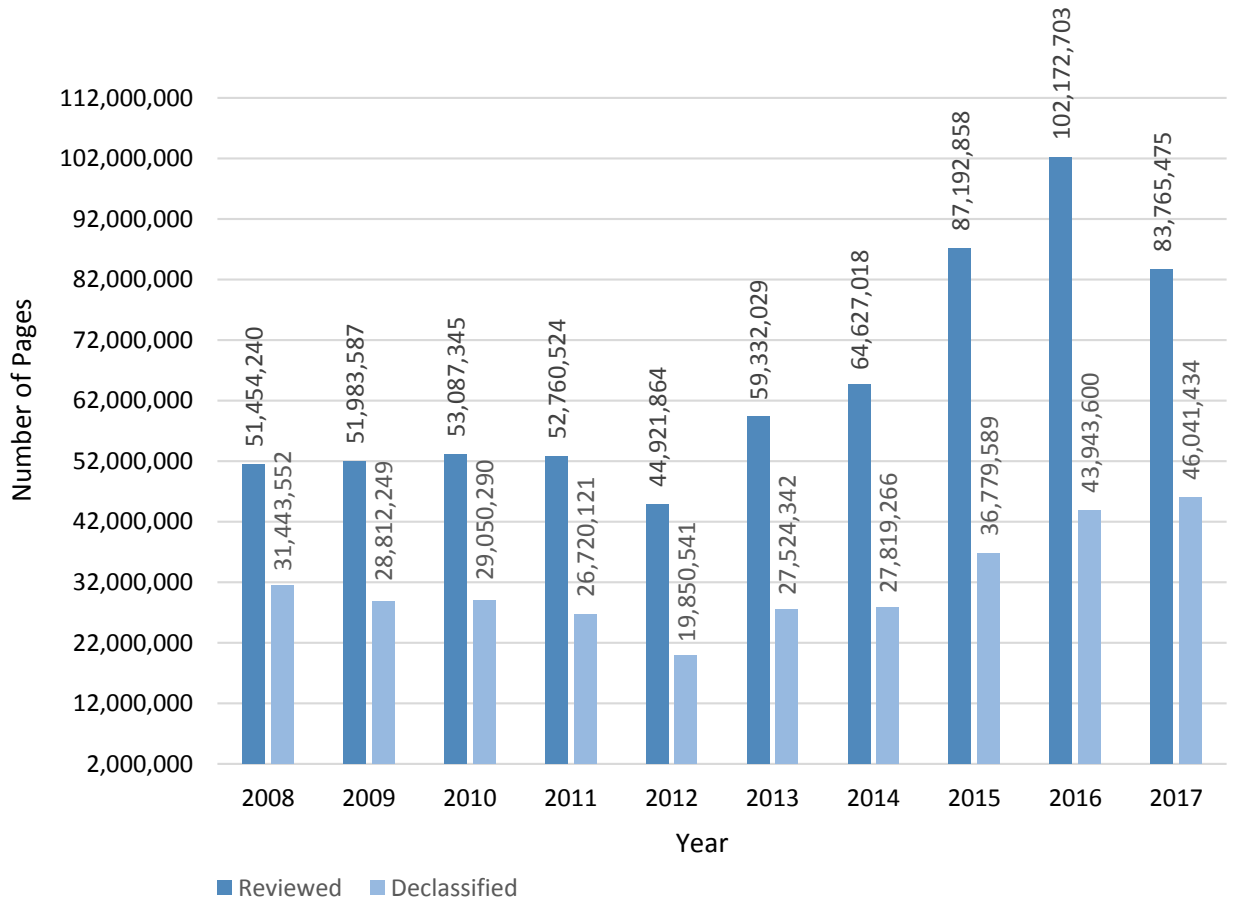
Derivative Classification Activity By Level of Classification

FY 1998–FY 2017

	Number of TOP SECRET Derivative Classification Decisions	Number of SECRET Derivative Classification Decisions	Number of CONFIDENTIAL Derivative Classification Decisions	TOTAL Number of Derivative Classification Decisions
1998	831,002	4,495,872	1,830,889	7,157,763
1999	742,488	5,724,197	1,402,172	7,868,857
2000	5,115,184	12,284,503	5,336,022	22,735,709
2001	5,521,184	10,521,394	4,885,040	20,927,618
2002	5,900,546	12,106,787	5,520,708	23,528,041
2003	1,756,506	9,557,153	2,680,309	13,993,968
2004	1,880,833	10,247,023	3,166,237	15,294,093
2005	1,560,713	9,898,420	2,489,007	13,948,140
2006	2,237,746	15,112,333	2,974,371	20,324,450
2007	2,655,430	16,904,233	3,308,955	22,868,618
2008	3,539,355	16,327,628	3,350,574	23,217,557
2009	19,069,896	30,125,909	5,455,960	54,651,765
2010	21,477,245	36,003,512	19,090,454	76,571,211
2011	26,058,678	51,650,067	14,356,117	92,064,862
2012	23,633,814	58,487,865	13,058,564	95,180,243
2013	19,441,385	51,659,131	9,023,873	80,124,389
2014	17,539,501	49,284,677	10,691,458	77,515,636
2015	9,679,301	36,206,472	6,892,581	52,778,354
2016	9,954,322	40,380,765	4,871,281	55,206,368
2017	9,615,440	36,115,335	3,710,737	49,441,512

Total Number of Pages Reviewed and Declassified*

FY 2008–FY 2017



* Excludes Mandatory Declassification Review

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

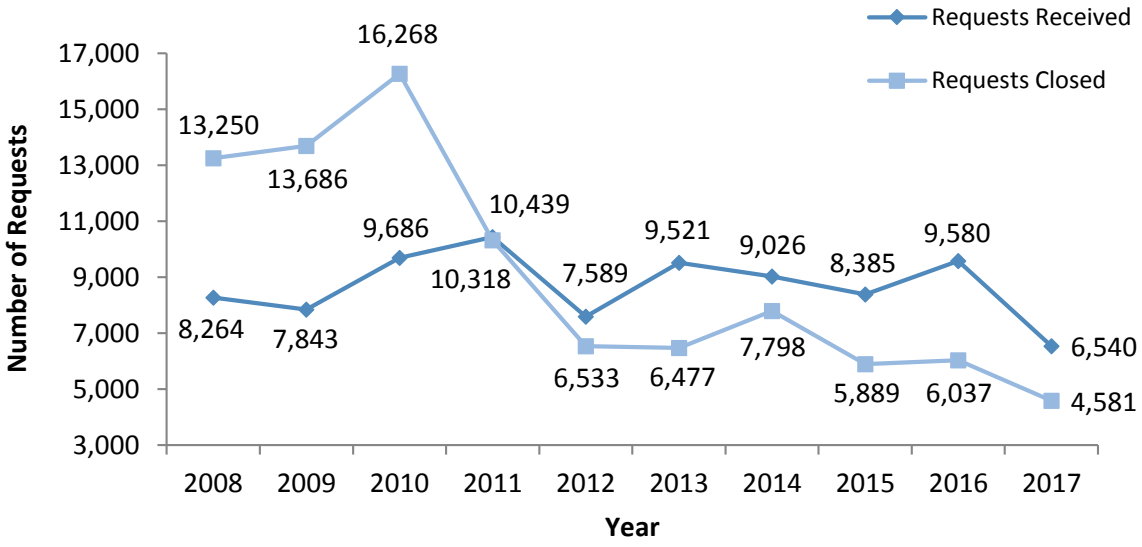
Number of Pages Reviewed and Declassified By Program

FY 2013–FY 2017

	Automatic			Systematic			Discretionary		
	Number of Pages Reviewed	Number of Pages Declassified	% Declassified	Number of Pages Reviewed	Number of Pages Declassified	% Declassified	Number of Pages Reviewed	Number of Pages Declassified	% Declassified
2013	52,470,623	25,771,199	49%	6,515,055	1,697,472	26%	346,351	55,671	16%
2014	60,491,810	25,660,183	42%	3,933,823	2,093,258	53%	201,375	65,825	33%
2015	84,424,836	36,042,022	43%	2,625,373	706,859	27%	142,649	30,708	22%
2016	96,577,037	39,608,944	41%	5,374,544	4,268,784	79%	221,122	65,872	30%
2017	83,014,284	45,776,310	55%	693,652	243,248	35%	57,539	21,876	38%

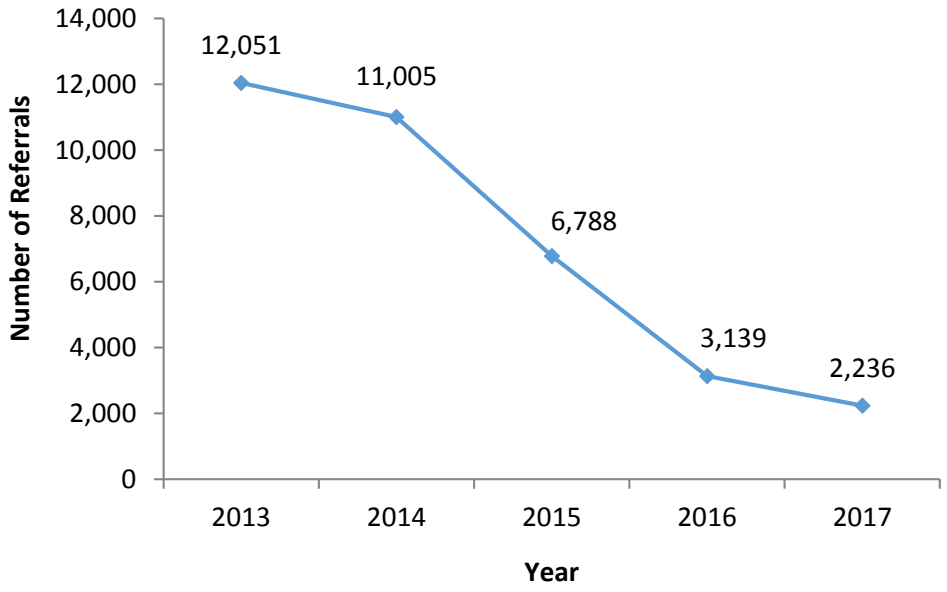
Mandatory Declassification Review Requests (MDR)

FY 2008–FY 2017



MDR Referred** Requests Received

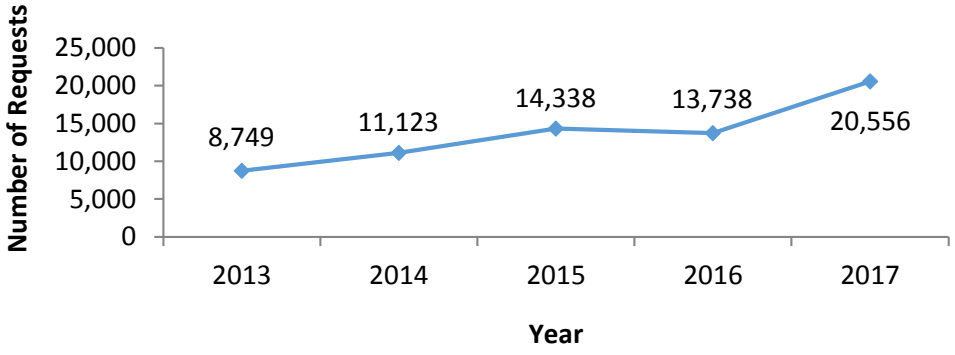
FY 2013–FY 2017



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

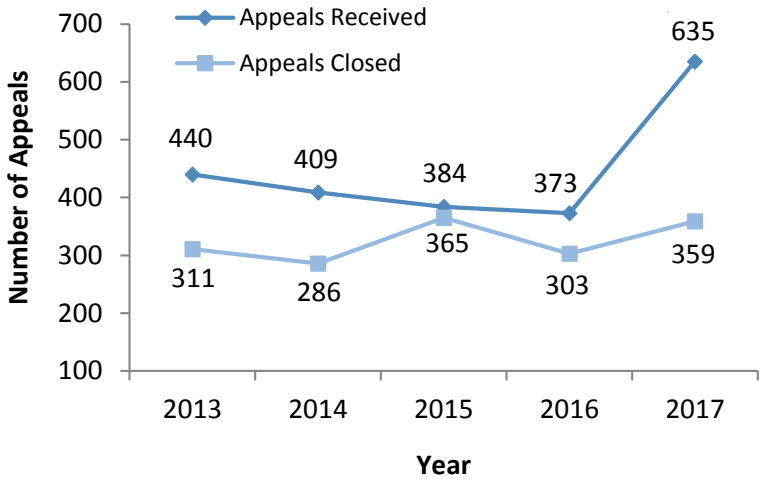
MDR Requests Unresolved for Over One Year

FY 2013–FY 2017



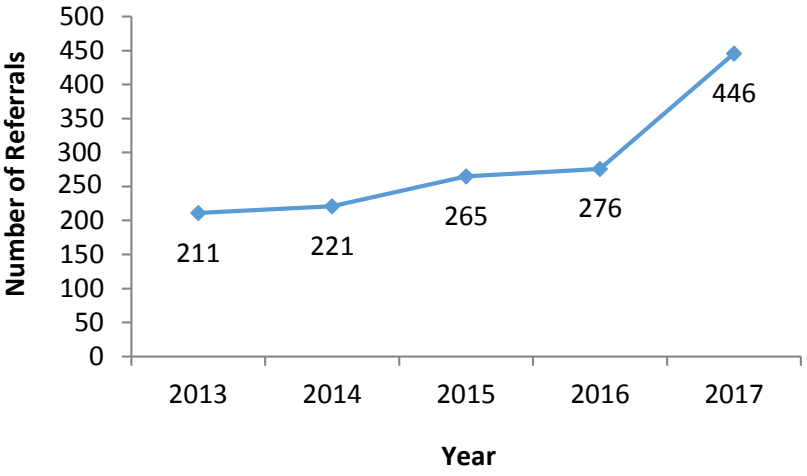
MDR Appeals

FY 2013–FY 2017



MDR Referred** Appeals Received

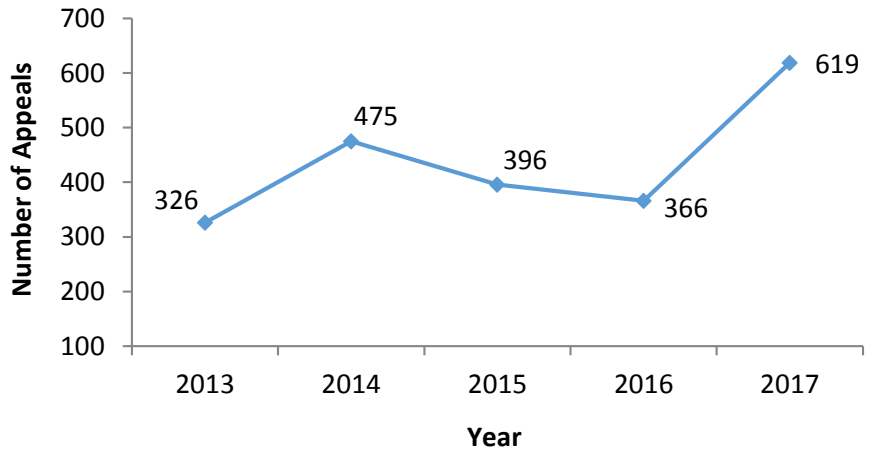
FY 2013–FY 2017



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

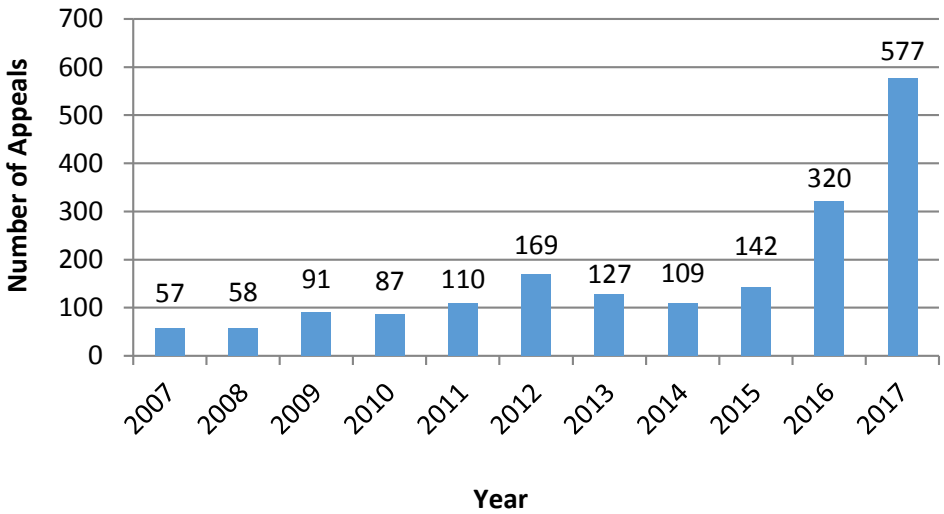
MDR Appeals Unresolved for Over One Year

FY 2013–FY 2017



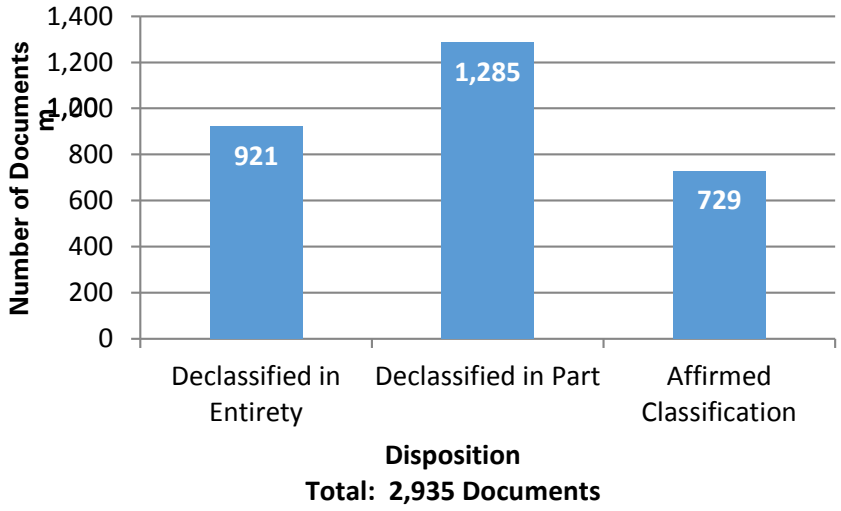
Number of Appeals Received by ISCAP

FY 2007–FY 2017



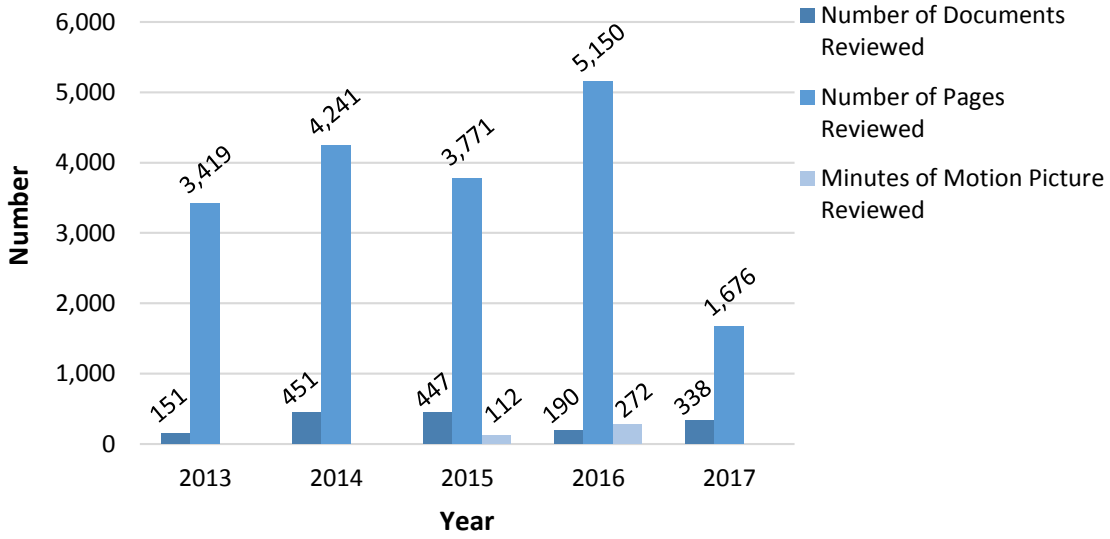
ISCAP Decisions

May 1996–September 2017



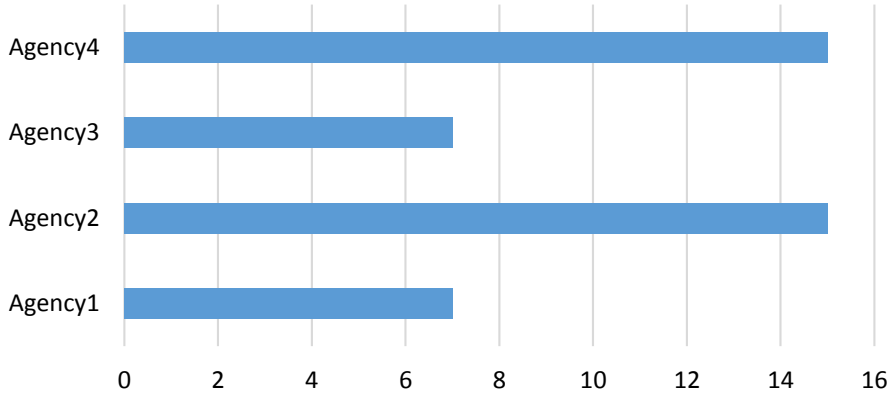
Comparison of ISCAP Activity

FY 2013–FY 2017



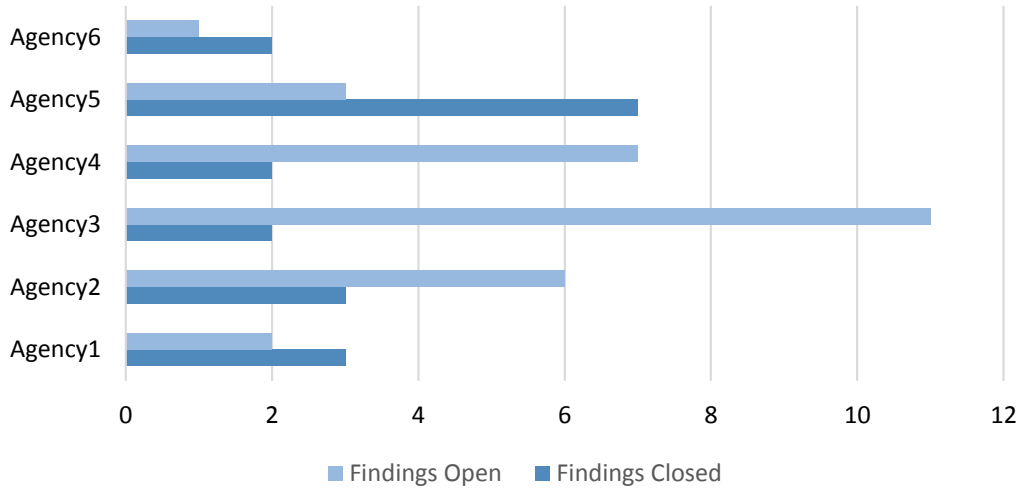
Full On-Site Review Findings

FY 2017



On-Site Follow-Up Review Findings

FY 2017



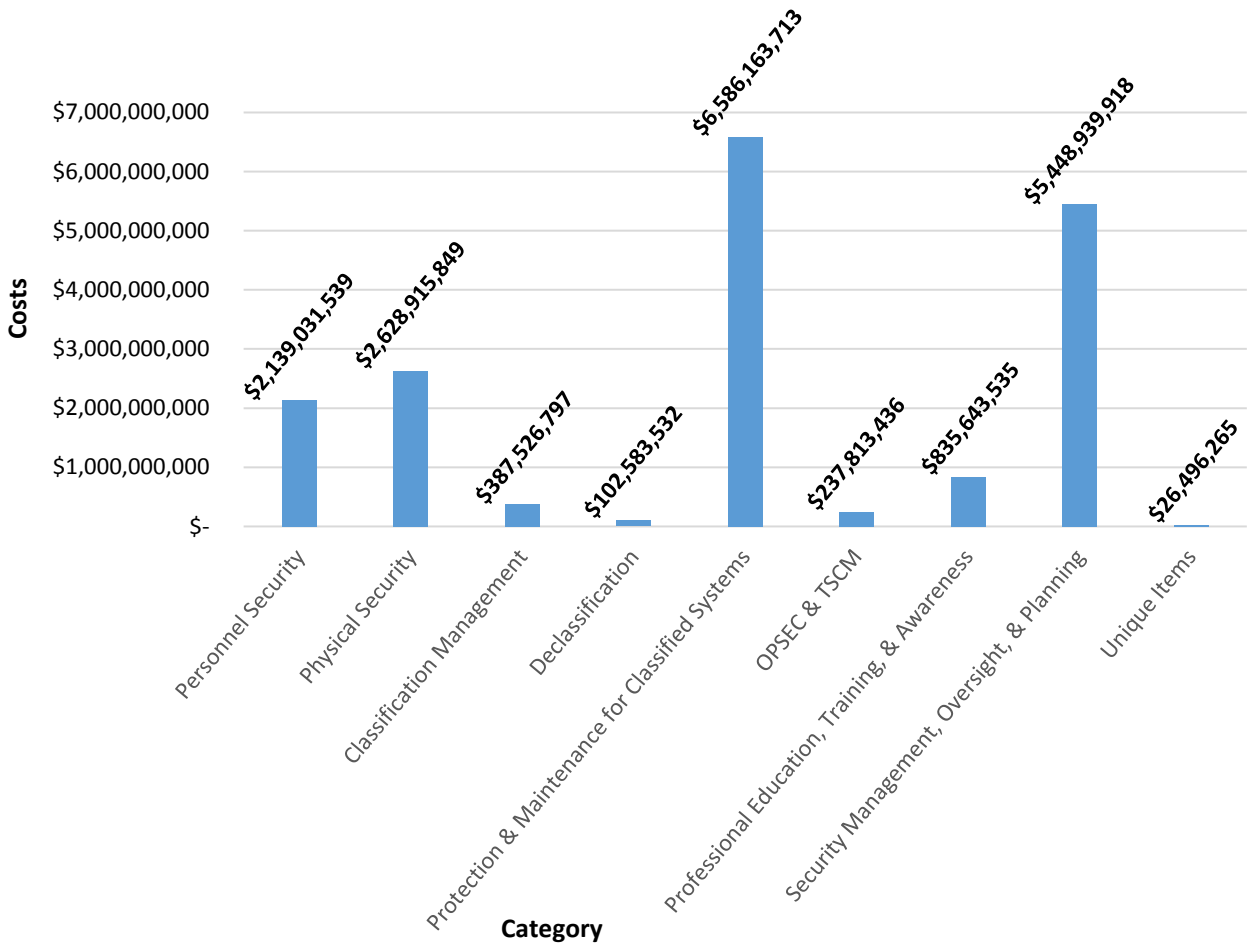
Frequently Occurring Document Discrepancies

FY 2017

Frequently Occurring Document Discrepancies	
"Classified By" Line	Documents did not include a "Classified By" line or did not have sufficient information on this line.
Multiple Sources	Documents, identified as being derived from multiple sources, did not have the list of sources on or attached to them.
Portion Marking	Documents did not include required portion markings.
Declassification	Documents did not include declassification instructions, or they had improper or incomplete declassification instructions.
"Derived From" Line	Documents did not include a "Derived From" line or did not include sufficient or appropriate information on this line, thus making it impossible to identify the source of the derivative classification.
Date of Origin	Documents did not identify their date of origin.
"Reason" Line	Documents, which were derivatively classified, improperly included a "Reason" line. This line may only be applied to originally classified documents.
Marking	Documents lacked overall classification markings or had improper overall classification markings.
Over-Classification	Documents, marked as classified, did not appear to contain information that, if disclosed, could reasonably be expected to cause damage to the national security.

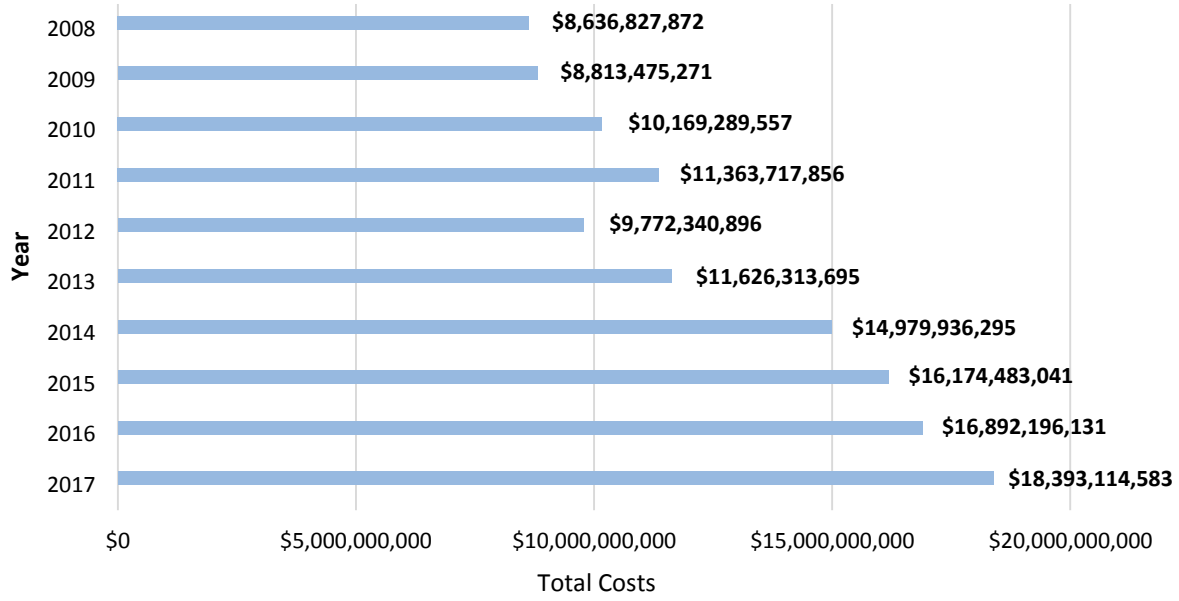
Government Security Classification Costs

FY 2017



Government Security Classification Costs

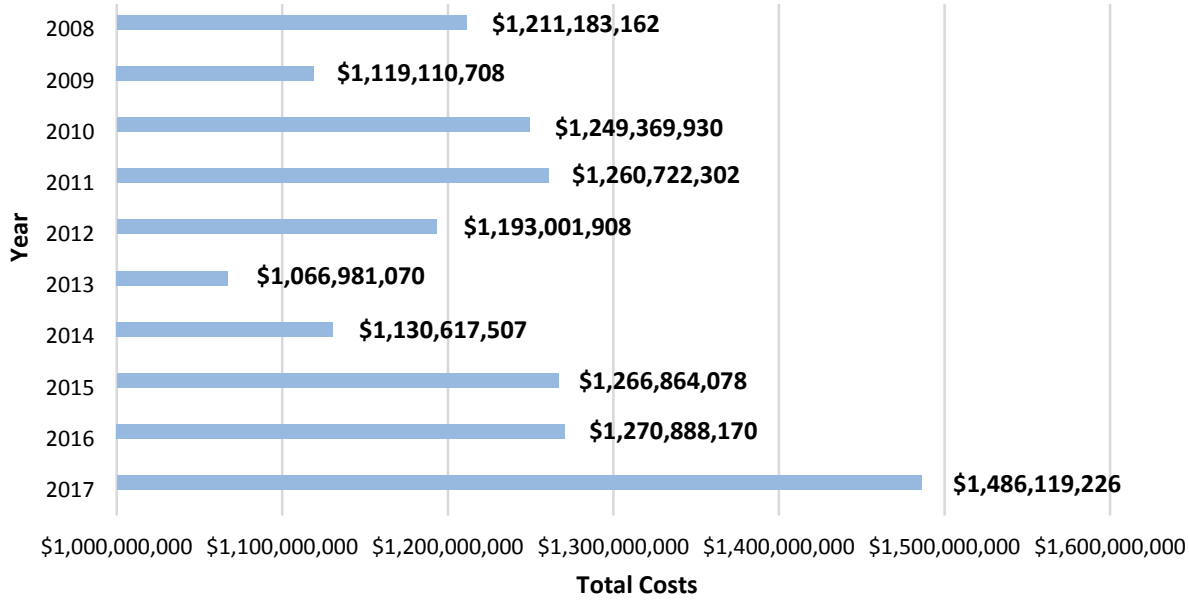
FY 2008–FY 2017



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

Industry Security Classification Costs

FY 2008–FY 2017



Controlled Unclassified Information (CUI)

FY 2017 Program Activity

GUIDANCE:

- December 6, 2016—ISOO issued a revised handbook on how to properly mark CUI, adding additional examples and clarifying guidance based on agency needs and requests.

- June 19, 2017—ISOO issued CUI Notice 2017-01 to provide agencies with recommendations regarding the implementation of the CUI Program.
  - This guidance addressed key programmatic elements, including: program management, training and awareness, physical safeguarding, information systems, destruction, self-inspections, incident management, and contracts and agreements.

- August 1, 2017—OMB issued Circular No. A-11 instructing agencies that estimates for FY 2019 should reflect consideration of Executive Order 13556 and the policies issued by the CUI Executive Agent, 32 CFR part 2002 and CUI Notice 2016-01.
  - ISOO collaborated with OMB on the development of this guidance.

- August 17, 2017—ISOO issued CUI Notice 2017-02 to provide agencies with recommendations on CUI destruction.
  - ISOO coordinated the issuance with the NIST in order to enhance agency cost-savings during the process of effectively destroying media.

OVERSIGHT:

- April 7, 2017—ISOO issued a memorandum to the heads of departments and agencies requiring an update on their implementation efforts.
  - This memorandum required agencies to submit their reports to the CUI Executive Agent by May 31, 2017.

- August 17, 2017—ISOO issued a memorandum to the heads of departments and agencies requiring that they submit their annual report to summarize their implementation efforts for FY 2017.
  - This memorandum required that agencies submit their reports to the CUI Executive Agent by November 1, 2017.

TRAINING:

- July, 2017—ISOO deployed a series of training modules to assist agencies in raising awareness of the CUI Program's implementation.
    - The training also provided a baseline for introductory training on the program's key elements (controlled environments, decontrolling, destruction, lawful government purpose, introduction to marking, and marking: non-traditional media).

- September 21, 2017—ISOO deployed a training module addressing unauthorized disclosures (prevention and reporting) in order to assist agencies with meeting training requirements for agency personnel on unauthorized disclosures of CNSI and CUI.

OUTREACH:

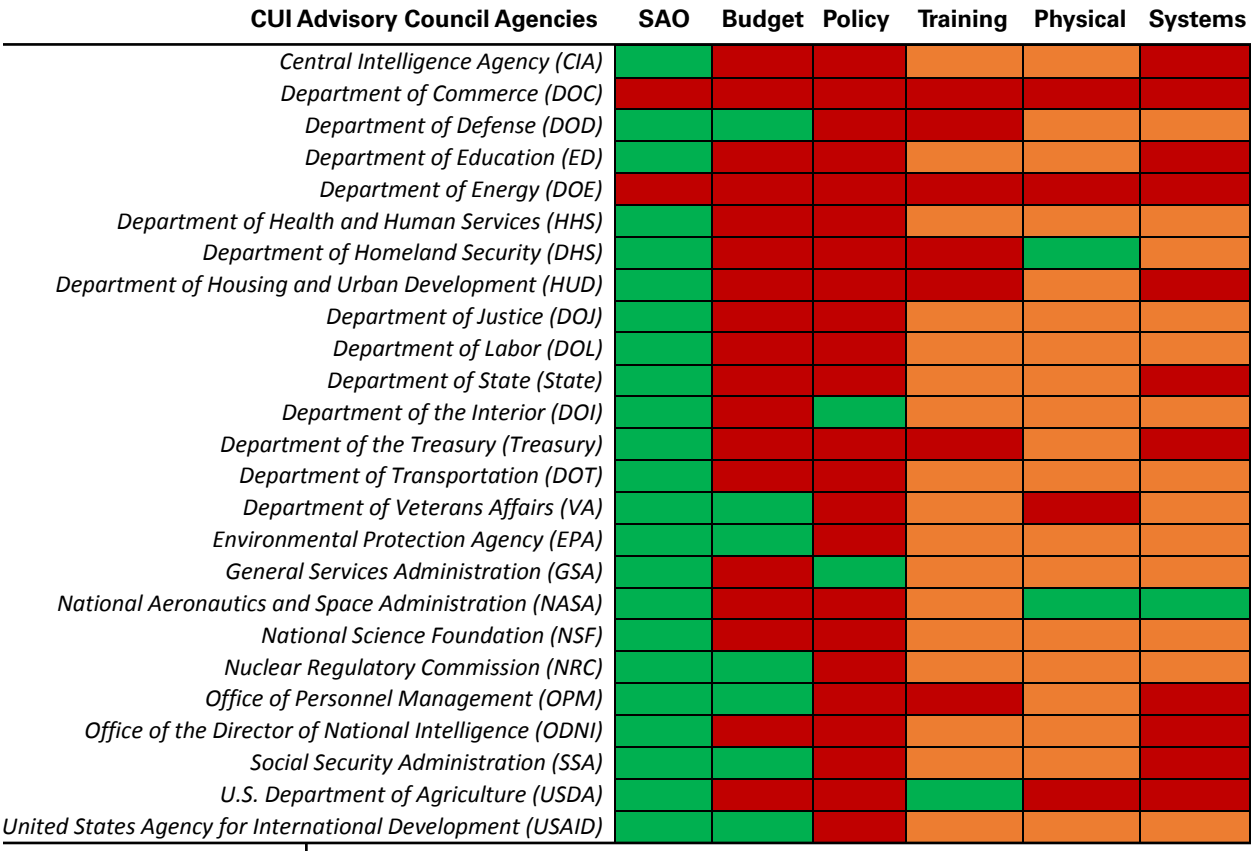
- Federal—ISOO provided over 50 briefings to Government entities ranging from cabinet-level agencies to boards and commissions.

- Non-federal—ISOO provided over 100 briefings to major industry associations and major contractors.
    - These briefings included State and local entities interested in preparing themselves for federal information-sharing and also adopting the model of the CUI Program for their own information management regimes.

Implementation Status of CUI Advisory Council Agencies

based on Annual Report Submissions for FY 2017

This chart reflects agency implementation efforts for FY 2017, based on completion of phased implementation requirements consistent with CUI Notice 2016-01. It does not reflect partial completion statuses, such as drafting, internal clearance, or planning.



SAO (Senior Agency Official) EO 13556	Green = SAO designated Red = SAO not designated
Budget (OMB)	Green = Budgeted for CUI Program implementation activities in FY17 or the agency plans to leverage existing resources for all implementation activities Red = Has not budgeted for CUI Program implementation activities in FY17
Policy (32 CFR Part 2002)	Green = Has reported that policy is completed Red = Policy is not completed
Training (32 CFR Part 2002)	Green = Has reported that the agency developed and deployed CUI training Orange = Has engaged in awareness activities (of the workforce or senior leaders) that addresses the CUI program and its implementation within the agency Red = Has not started or engaged in any awareness or training activity related to the CUI Program
Physical (32 CFR Part 2002)	Green = Has reported that the agency assessed and modified all physical environments to be suitable for storing and handling CUI Orange = Is either planning, assessing, or modifying physical environments to align with the standards of the CUI Program Red = Has not taken any steps to verify (plan or assess) the physical environments where CUI is handled or processed
Systems (32 CFR Part 2002)	Green = Has reported that all systems meet the standards of the CUI Program (i.e., the moderate confidentiality baseline) Orange = Has reported that the agency has a plan to set up a process to inventory, assess, and modify systems that store, process, or transmit CUI or has started identifying or assessing systems Red = Does not have a plan to inventory, assess, and modify systems that store, process, or transmit CUI or has not started assessing agency systems that that store, process, or transmit CUI