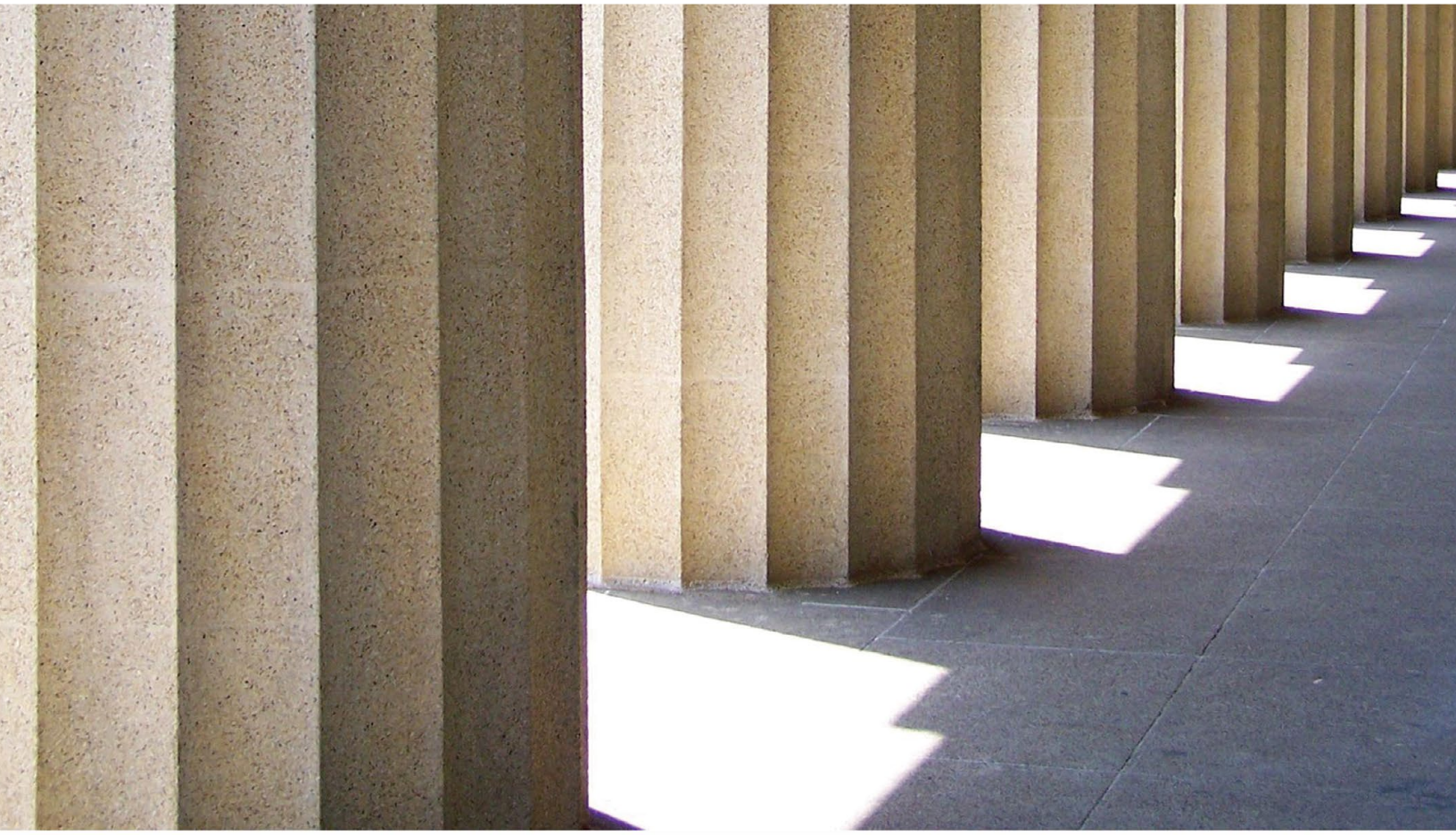
Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY



Council of the Inspectors General on Integrity and Efficiency (CIGIE) Summary Report of Inspectors General Efforts Under the Evaluation of the Implementation of Public Law 111-258, "Reducing Over-Classification Act"

August 2019

This report was
prepared on behalf of the
Council of the Inspectors General
on Integrity and Efficiency

RESULTS IN BRIEF

Council of the Inspectors General on Integrity and Efficiency (CIGIE) Summary Report of Inspectors General Efforts Under the Evaluation of the Implementation of Public Law 111-258, "Reducing Over-Classification Act"

Objective

The objective of this report is to summarize key findings identified in 2013 reports and in 2016 followup reports produced by 13 Federal agency Offices of Inspectors General (OIGs) regarding original and derivative classification and Classified National Security Information (CNSI) program management. This summary was produced in response to a request from the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Background

Public Law 111-258, "Reducing Over-Classification Act," requires that the Inspector General (IG) of each department or agency of the United States with an officer or employee who is authorized to make original classifications (the original classification authority [OCA]) carry out evaluations of that department or agency or a component of the department or agency:

- to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and
- to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

This summary report highlights key findings in the 13 participating OIGs' individual reports. Also, where applicable, this report summarizes improvements made between 2013 and 2016 in the areas of original classification, derivative classification, and general program knowledge.

Summary of Findings

The following is a summary of the key findings and progress reported by the 13 OIGs.

Original Classification — The 2013 and 2016 reports revealed common issues related to OCAs, program knowledge, coordination of security classification guides (SCGs), and SCG accuracy and completeness. In 2013, 9 of the 13 OIGs reported that OCAs at their agencies were appropriately designated, were knowledgeable of classification requirements, and were appropriately trained for their positions. However, a sampling of 472 SCGs reviewed by 5 of the 13 OIGs in 2013 and 3 of the 13 OIGs in 2016 found that most SCGs in 4 of the 5 agencies were missing required elements, such as guidance on the proper process and points of contact to challenge incorrect classification, needed for derivative classifiers to make proper derivative classification decisions.

Derivative Classification — In 2013, all 13 OIGs' reports addressed discrepancies in derivative classification. The OIGs attributed the discrepancies to problems with document reviews, derivative classifier input, and Classification Management Tool (CMT—an automated tool that allows the user to apply correctly formatted classification markings to electronic documents) shortfalls that adversely affected derivative classification. In 2016, that number decreased to 11 of 13. The OIGs also identified derivative classification problems related to inconsistent standards within agencies, disparate marking methods employed by derivative classifiers, and inaccurate and outdated agency CMTs that support the classification marking process.

Program Management — In 2013, 5 of the 13 OIGs found that their agencies had not adopted applicable classification policies, procedures, rules, and regulations. By 2016, 2 of the 13 OIGs found that their agencies still had not adopted them. In 2013, 11 of the 13 OIGs found that their agencies did not fully follow or effectively administer applicable classification policies, procedures, rules, and regulations as required. In 2016, 7 of the 13 OIGs found that their agencies had not done so. In 2013, 5 of the 13 OIGs found instances of over-classification. In 2016, 3 of the 13 OIGs still found instances of over-classification.

In both 2013 and 2016, only one OIG found that its agency had a strong Classified National Security Information (CNSI) program. The other 12 OIGs identified challenges in the following areas:

- ***Security Education and Training*** — In 2013, 7 of the 13 OIGs addressed concerns with OCA training. According to the 2013 reports, most OCAs received training as prescribed; however, curriculum and training updates in policy were still being developed and refined to align with Executive Order 13526. In 2016, only two OIGs identified concerns with OCA training. Similarly, in 2013, 9 of the 13 OIGs identified concerns with derivative classifier training. In 2016, only three OIGs identified such concerns. In both 2013 and 2016, a few OIGs also determined that CMT training could be improved to enhance classification marking in the electronic environment. None of the OIGs identified an occurrence when its agency suspended original or derivative classification authority for employees failing to meet training requirements.
- ***Security Self-Inspection Program*** — In 2013, 10 of the 13 OIGs identified discrepancies in their agencies self-inspection programs. Specifically, the OIGs identified issues with sampling of documents, records management, frequency of CNSI program reviews, resource constraints, and policies. Although agencies implemented corrective measures, in 2016 10 of the 13 OIGs still identified discrepancies within five general areas of concern—sampling, records management, frequency of reviews, resource constraints, and policy.
- ***Security Reporting*** — In 2013, 10 of the 13 OIGs identified discrepancies in Standard Form (SF) 311 reports with respect to the manner in which statistics were compiled and the reliability of information reported.[1] For example, agencies compiled data using different assumptions about what should be included and employing disparate methods for collecting and estimating data. Although some agencies implemented corrective measures in 2016, 7 of the 13 OIGs still identified issues in four general areas of concern—methodology, verification, guidance, and calculations. OIG reviews also found inconsistent applications of the Information Security Oversight Office's (ISOO) requirements and inconsistent definitions of what annual reports should include.[2]

[1] The SF 311, "Agency Security Classification Management Program Data," is the data collection form that every Executive branch agency submits annually to report the number of OCAs, classification decisions, mandatory review requests, and declassification decisions for that agency.

[2] The ISOO is responsible for policy and oversight of the Government-wide security classification system and the National Industrial Security Program. The ISOO is a Component of the National Archives and Records Administration and receives policy and program guidance from the National Security Council.

- ***Performance Evaluations*** — In 2013, 5 of the 13 OIGs identified problems with how agency personnel were evaluated. The five determined that some agency components included a critical element on security in employees' performance evaluations, while other components did not. The OIGs found that this longstanding requirement had not been enforced. In 2016, 3 of the 13 OIGs still identified discrepancies, while 9 of the 13 OIGs did not address the issue. One OIG found improvement.
- ***Challenges to Classification*** — In 2013, 4 of the 13 OIGs determined that policy and training on the process for formally or informally challenging improperly classified documents needed to be strengthened. One OIG determined that agency personnel knew the process of formally or informally challenging document classification. In 2016, only three OIGs addressed classification challenges. One OIG identified improvement. The remaining two OIGs identified improved processes, but determined that some aspects of policies at these two agencies still needed to be updated.
- ***Incentives and Sanctions*** — Public Law 111-258, section 6(a), allows agencies to provide incentives to employees for classifying documents appropriately and for challenging classification decisions that employees believe are improper. In both 2013 and 2016, no OIG identified an occurrence when its agency provided incentives to employees for accurate classification. Moreover, no OIG reported on the imposition of agency sanctions for inappropriate classification decisions or noncompliance.

CONTENTS

Introduction

Summary of Findings

Appendixes

Council of the
INSPECTORS GENERAL
on INTEGRITY *and* EFFICIENCY

INTRODUCTION

Objective

The objective of this report is to summarize key findings identified in 2013 reports and in 2016 followup reports produced by 13 Federal agency Offices of Inspector General (OIGs), regarding original and derivative classification and Classified National Security Information (CNSI) program management.[3] This summary was done in response to a request from the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Background

The National Commission on Terrorist Acts Upon the United States observed that the "over-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholders and public access to information."[4]

From 2013 to 2016, the following 13 OIGs, in consultation with the Information Security Oversight Office (ISOO), audited and evaluated their agencies' implementation of CNSI programs: Agriculture, Commerce, Defense, Energy, Environmental Protection Agency, Health and Human Services, Homeland Security, Justice, Nuclear Regulatory Commission, State, Transportation, the Treasury, and the U.S. Agency for International Development.[5] The audits and evaluations covered core program elements, such as program management, classification and marking, security education and training, and self-inspections.[6]

---

[3] Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified. Information may be derivatively classified in two ways: (1) through the use of a source document, usually correspondence or a publication generated by an original classification authority; or (2) through the use of a security classification guide. Classification guides provide consistency and accuracy to classification decisions. Every derivative classification action is based on information for which classification has already been determined by an original classification authority. Derivative classification decisions must be traceable to the original classification decision made by an original classification authority.

[4] We have used a working definition of "over-classification" that the ISOO supplied: the designation of information as classified, when the information does not meet one or more of the standards for classification under section 1.1 of Executive Order 13526. In other words, over-classification is either treating unclassified information as if it were classified, or classifying information at a higher level than is appropriate.

[5] Classified National Security Information is information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status.

[6] Executive Order 13526, section 5.4(d)(4), requires that the component Senior Agency Official establish and maintain an ongoing self-inspection program, including regular reviews of representative samples of the agency's original and derivative classification actions. Self-inspections also evaluate the effectiveness of agency programs covering declassification, safeguarding, security violations, security education and training, and management and oversight. The results are reported annually to the ISOO.

Although one OIG determined that its agency had a well-developed, effective, and properly implemented CNSI program, all 13 OIGs reported that their agencies had CNSI program areas that required attention in order to meet the requirements of Executive Order 13526.[7]

This summary report provides the status of the 13 agency CNSI programs in 2013 and 2016, as reflected in the OIGs' reports. We compiled this report using a summary of the results of the 13 individual OIG audits and evaluations. In total, the 13 participating OIGs issued 29 reports related to the implementation of the CNSI program in their agencies. We used only the 29 reports to gather information for this summary report. The OIGs did not offer, nor did we request, additional information.

Public Law 111-258, section 6(b), required the OIGs to complete an initial evaluation by September 30, 2013, discussing the results of the evaluation of the effectiveness of policies, procedures, rules, regulations, and management practices that may be contributing to persistent misclassification and over-classification. The law also required the OIGs to complete a second evaluation or audit by September 30, 2016, reviewing the progress made pursuant to the results of the first evaluation. This summary report contains the results of those audits and evaluations.

In addition, Public Law 111-258, section 6(b)(3)(C), required the OIGs to coordinate with one another and with the ISOO to ensure that the OIG audits and evaluations followed a consistent methodology, as appropriate, that allows for cross-agency comparisons.

In 2013, the CIGIE created an evaluation guide to promote consistency of evaluations conducted under Public Law 111-258.[8] The working group that developed the evaluation guide included 11 of the 13 OIGs whose audits and evaluations are summarized in this report, as well as OIGs from the Defense Intelligence Agency, Intelligence Community, National Geospatial-Intelligence Agency, National Reconnaissance Office, and National Security Agency.

[7] Executive Order 13526, issued by the President on December 26, 2009, prescribes a uniform system for classifying, safeguarding, and declassifying national security information.

[8] For the 2013 evaluation, an evaluation guide that a working group of participating OIGs, led by the DoD OIG, prepared for all OIGs participating in this Government-wide effort in response to a request from the CIGIE. The evaluation guide was intended to meet Public Law 111-258 requirements regarding the responsibilities of each participating department and agency. The working group was formed to ensure consistency in the evaluative process, comparable reporting, and the ability to compare results across agencies. The evaluation guide is on the CIGIE website: https://www.ignet.gov/content/reports-publications (under "List by Year," then "2013"), "A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the Reducing Over-Classification Act."

Fundamental Classification Guidance Review

Executive Order 13526, section 1.9, directed agency heads to complete, on a periodic basis, a comprehensive review of the agency's classification guidance, particularly security classification guides (SCGs), to ensure that the guidance reflects current circumstances.[9] Executive Order 13526 also required that the review, known as the Fundamental Classification Guidance Review (FCGR), evaluate classified information to determine whether it meets the standards for classification or should be declassified. The FCGR must include input from original classification authorities (OCAs) and agency subject matter experts to ensure a broad range of perspectives.

In accordance with Title 32 Code of Federal Regulations (CFR) Part 2001, the implementing directive of Executive Order 13526, section 2001.16, the initial FCGR was completed by July 2012. Agency heads provided a report summarizing the results of each FCGR to the ISOO and released an unclassified version to the public except when the existence of the guide or program was itself classified.

Participating OIGs then reviewed agency FCGR results before completing their 2013 reports required by Public Law 111-258, section 6(b)(2)(A), incorporating FCGR findings where relevant. According to 32 CFR section 2001.16, additional FCGRs must be completed at least every five years thereafter. Agencies provided FCGR status updates in October 2016 and February 2017. Final FCGR reports were submitted to the ISOO by June 30, 2017. The 2017 FCGR tasking memorandum, checklist, progress updates, and agency FCGR summary reports are available at: https://www.archives.gov/isoo/fcgr/2017-fcgr.html.

Overview of Areas for Summary Review

Public Law 111-258, section 6(b)(3)(C), required that IGs who are required to carry out these evaluations coordinate with one another and with the ISOO to ensure that evaluations follow a consistent methodology, as appropriate, that allows for cross-agency comparisons.

Adhering to the general methodology, cross-agency comparisons were possible along the following general issue areas: original classification, derivative classification, and program management.

[9] SCGs contain a set of classification instructions from an OCA to derivative classifiers. These instructions identify elements of information on a specific subject that must be classified and the classification level and duration for each element.

SUMMARY OF FINDINGS

Original Classification

The 2013 and 2016 reports revealed common issues related to OCAs, program knowledge, coordination of SCGs, and SCG accuracy and completeness. In 2013, 9 of the 13 OIGs reported that OCAs at their agencies were appropriately designated, were knowledgeable of classification requirements, and were appropriately trained for their positions. However, according to OIG reports, some agencies needed to review positions to confirm the need for OCAs. Also, a sampling of 472 SCGs reviewed by 4 of the 13 OIGs in 2013 and 2 of the 13 OIGs in 2016 found that most of the reviewed SCGs were missing required elements needed for derivative classifiers to make proper derivative classification decisions. The OIGs determined that guidance was needed to address missing or inaccurate declassification dates, proper use of dissemination control and handling markings, and the proper process and points of contact for challenging classification.

Original Classification Authorities

This section highlights findings from OIG reports in 2013 and 2016 specific to OCA designations, knowledge, and guidance. The OIG reports addressed three common themes: the designation of OCAs, the sufficiency of OCA program knowledge, and the accuracy of SCGs.

Agency heads are required to properly designate OCAs in accordance with Executive Order 13526, section 1.3. This authority can be delegated further if there is a demonstrable and continuing need for other officials to exercise the authority.[10]

OIGs interviewed OCAs to evaluate the OCAs' knowledge of classification management procedures. The intent of these interviews was to determine whether the position held by the OCA was required by the agency and to assess whether the OCA had sufficient expert knowledge of the information and classification requirements for the appropriate classification of information.

[10] Not every Federal agency has an OCA. The 13 federal agencies whose OIGs participated in this effort do have an OCA, and depending on the size of the organization, may have several OCAs delegated to perform original classification duties.

Additionally, OIGs reviewed SCGs to ensure that guidance in the SCGs reflected current circumstances and to identify classified information that no longer required protection and could be declassified. The problems identified by each OIG during its reviews of the agencies' original classification programs are summarized in the following table.

Table 1. Agency OIG Reviews of Original Classification Authorities

Dept./ Agency	Identified Issue(s)		OCA Designations		Program Knowledge		SCG Reviews	
	2013	2016	2013	2016	2013	2016	2013	2016
DoD	X	X	✓	X	X	X	X	X
DHS	✓	N/A	✓	N/A	✓	N/A	✓	N/A
DOC	X	N/A	✓	N/A	X	N/A	N/A	N/A
DOT	✓	✓	✓	✓	✓	✓	N/A	N/A
Energy	✓	N/A	✓	N/A	✓	N/A	N/A	N/A
EPA	X	X	✓	N/A	X	X	X	X
HHS	X	✓	N/A	✓	X	✓	N/A	N/A
Justice	X	✓	X	✓	X	✓	X	✓
NRC	X	✓	N/A	N/A	X	✓	N/A	N/A
State	✓	X	✓	X	N/A	N/A	N/A	N/A
Treasury	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
USAID	X	X	✓	N/A	X	X	N/A	N/A
USDA	X	X	✓	N/A	X	X	X	N/A

Legend: X – Issue(s) identified; ✓– No Discrepancy; N/A – Not addressed

Sources: Participating OIG reports as listed in Appendix B.

Agencies (as listed): Department of Defense; Department of Homeland Security; Department of Commerce; Department of Transportation; Department of Energy; Environmental Protection Agency; Department of Health and Human Services; Department of Justice; Nuclear Regulatory Commission; Department of State; Department of the Treasury; U.S. Agency for International Development; U.S. Department of Agriculture.

Original Classification Authority Designation

Agency heads are responsible for ensuring that designated subordinate officials have a required and continuing need to exercise original classification authority. OIGs reported that on a recurring basis, some agencies took steps to reduce OCA positions that were no longer required.

2013

In 2013, 9 of the 13 OIGs reported that OCAs in their agencies were appropriately designated; three OIGs did not address the issue. However, the Department of Justice (DoJ) OIG expressed concern with the appropriate delegation of OCA authorities. The OIG identified an inordinately high number of original classification decisions in one component and determined that the numbers were inconsistent with the component's mission. The OIG also found a high ratio of derivative classifiers to OCAs in the same component. The OIG determined that classification decisions reported as original classification decisions were instead derivative classification decisions. Based on these findings, the OIG recommended a review of OCA positions throughout the agency.

The Department of Homeland Security (DHS) OIG found that the agency head, in accordance with Federal guidance, designated OCAs to determine the original classification of documents. The OIG also determined that the OCAs were following processes described in Executive Order 13526 and 32 CFR section 2001.11 for making original classification decisions.

The Department of Commerce (DoC) OIG noted that agency leadership directed a review of OCA positions to verify the need for the positional authority. Based on that review, the agency reduced the number of OCA positions from 16 to 3.

The Department of Defense (DoD) OIG noted that OCAs were properly designated, were knowledgeable of classification requirements to ensure that information is not over-classified, received training, and relied heavily on their security personnel. The OIG also highlighted the low number of classification decisions by OCAs. The OIG recommended a review of OCA positions, noting that it was necessary to remove inherited authorities from positions that had evolved or changed to a point that they no longer required the delegated authorities.

The Environmental Protection Agency (EPA) OIG found that the EPA had only one position with original classification authority. The OIG determined that it was appropriate for only one position to have original classification authority, without the ability to delegate the authority to other positions.

2016

After 9 of the 13 OIGs found in 2013 that their agencies appropriately designated OCAs, only five OIGs addressed OCA designations in their 2016 reports.

In response to a 2013 DoD OIG report recommendation, the DoD issued an April 16, 2015, memorandum to its components directing them to validate each OCA position and to assess whether that position was still required. As a followup, the OIG conducted surveys to gauge the level of compliance. Of 106 security managers who responded to the survey, only 15 had conducted the requisite review.

The DoJ OIG determined that in response to its 2013 report on the high number of OCAs, the agency decreased the OCA count from 64 to 46. The OIG also referenced a 2013 finding that derivative classification determinations had been improperly identified as original classification decisions. To address this error, the agency issued a formal memorandum to components explaining the importance of understanding the differences between original and derivative classification decisions. As a result of agency efforts, in FY 2015 the annual number of original classification decisions decreased to zero.

The Department of State (DoS) OIG compared a list of positions authorized as Top Secret OCAs and Secret OCAs with lists of all of the security-cleared agency employees as of September 30, 2015. The combined list of 910 OCA positions did not correspond with the 2014 count of 999 positions reported to the ISOO. The SF 311 count had been consistent over a 4-year period. The OIG determined that the difference of 89 OCA positions was attributable, in part, to changes in the organizational structure and staffing changes. The OIG reported that agency standard operating procedures did not address keeping the lists of OCA positions up to date. The OIG recommended establishing a process to periodically review and update OCA lists, as necessary.

Program Knowledge

OCAs may classify only that information which is under their area of responsibility, such as a specific project, program, or type of operation. The participating OIGs conducted surveys and reviews to determine whether individuals with OCA designations had expert knowledge of classification requirements and to evaluate whether programs were effectively administered to support classification decisions.

2013

In 2013, 8 of the 13 OIGs found discrepancies with aspects of OCA program knowledge, three OIGs found no discrepancies, and the remaining two OIGs did not address the issue. In one example of an identified discrepancy, the Department of Health and Human Services (HHS) OIG reported that originally classified documents met most requirements; however, some documents lacked portion markings on various pages and paragraphs. Specifically, two documents were missing the required paragraph markings, one was missing the required page markings, and one was missing both. Portion markings indicate which portions are classified and which are unclassified within the same document. Portions are marked separately to avoid over-classification.

OIGs also identified deficiencies in classification guidance. The DoD OIG determined that SCGs were missing elements required to assist derivative classifiers with derivative classification decisions. The U.S. Agency for International Development (USAID) OIG found that the agency did not use an SCG and did not update parts of its classification policy. The agency instead used an SCG from another organization with a related mission. The EPA had no approved SCGs, the EPA OIG found, even though the OCA had taken original classification actions, classifying seven documents over the course of seven years.

The DoJ OIG determined that agency components with OCAs did not coordinate effectively when they developed program-specific SCGs. Along similar lines, the DoD OIG found SCGs that did not contain point of contact information or the requisite forms needed to help derivative classifiers resolve questions about classified information. The DoJ and EPA OIGs identified improperly marked originally classified documents.

2016

In 2016, 4 of the 13 OIGs again found discrepancies with aspects of program knowledge.

In 2013, the EPA OIG found seven originally classified documents with no corresponding SCGs. The OIG recommended that the agency prepare, review, and approve appropriate SCGs and distribute them to users of the originally classified information. During the 2016 review, the EPA OIG found that the agency completed corrective actions to address all recommendations except for two related to SCGs. Of these two outstanding recommendations, the first calls on the agency to ensure the preparation, review, and approval of appropriate SCGs, while the other recommended that the agency ensure the distribution of SCGs to users of the agency's originally

classified information. The original milestone date for finalizing an SCG approval process was September 30, 2014. According to the agency, an SCG was expected to be completed and approved by the Administrator within FY 2016.

The HHS OIG, which identified improperly marked originally classified documents in its 2013 report, found that the agency took appropriate action to address portion-marking issues in accordance with the original recommendations. However, the OIG identified an originally classified document issued in 2015 that did not include the reason for classification as required by Executive Order 13526. The agency addressed this error by correcting the document and reinforcing training.

The USAID OIG, whose agency did not have an SCG or associated policy in 2013, noted that the agency addressed the finding before the 2016 review. In 2016, however, the OIG identified systemic issues with respect to overall program management. The SCG did not contain the required point of contact information. Moreover, the classification policy did not meet the requirements prescribed in Executive Order 13526.

During the 2013 audit, the U.S. Department of Agriculture (USDA) OIG identified two approved originally classified documents. However, neither document had been properly marked with the OCA's identification or the reason for classification. Because of the infrequency of original classification decisions, the OIG recommended creating a checklist that would outline the required markings to help the OCA ensure that originally classified documents were appropriately marked. In response, the agency developed a desktop reference guide and flowchart for OCA use. The OIG's review of the desktop reference in 2016 determined that the flowchart assisted with classification determinations, but did not provide sufficient guidance on classification markings. The agency provided the OIG with a revised chart that identified some required markings for originally classified documents, but did not include the requirements for portion markings or overall classification markings.

Security Classification Guide Sample Reviews

Individuals with OCA designations create security classification guides (SCGs) to provide a set of instructions to derivative classifiers. These instructions identify elements of information on a specific subject that must be classified, and define the classification levels and durations for those elements.

Executive Order 13526, section 1.9, directs agency heads to complete, on a periodic basis, a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure that the guidance reflects current circumstances

and to identify classified information that no longer requires protection and can be declassified. In 2012, to comply with Executive Order 13526, agencies conducted an initial FCGR to begin the comprehensive review process.[11]

Five OIGs in 2013 and three in 2016 reviewed a total of 472 SCGs, to assess whether OCAs were effectively making classification determinations and to gauge SCG alignment with Executive Order 13526.

2013

In 2013, five agencies reported on discrepancies found during SCG reviews and 8 agencies did not address the issue. The remaining agency, DHS OIG determined that the eight SCGs it reviewed at its agency complied with all policies, procedures, rules, and regulations related to SCGs. The OIG found that central security office guidance to the components to make their SCGs uniform led to a reduction in SCGs for the agency. As of July 2012, the agency had 45 SCGs, down from 74 the previous year. The eight SCGs that were reviewed contained information related to the types, topics, reasons, levels, and duration of classifications, as described in Executive Order 13526. All SCGs reviewed were signed by an OCA delegated by the Senior Agency Official (SAO).[12] The central security office maintained an index of all agency-published SCGs. The security office initiated a review of SCGs at least every 5 years in accordance with 32 CFR section 2001.16(a).

The DoD OIG found that SCG template instructions for those who wanted to challenge classification were not consistent with the intent of Executive Order 13526, section 5.3. Agency policy did not require SCGs to contain language that encourages challenges and provides appropriate information to assist in the challenge process. The OIG also found that less than 44 percent of the SCGs it reviewed contained a required form used to identify a change to the SCG. Also, 55 percent of the SCGs reviewed still referenced Executive Order 12958, which was superseded by Executive Order 13526, as the basis for classification, regrading, or declassification of information. Additionally, 4.7 percent of the SCGs contained declassification dates that had already passed.

[11] The FCGR program was created on December 29, 2009, under Executive Order 13526. According to the ISOO, the review serves as a guide and benchmark for Federal agencies to ensure proper classification of information vital to national security, while expediting declassification by avoiding over-classification and unnecessary withholding of records. Accurate and current SCGs also ensure standardized classification within and across Federal agencies. All Federal agencies with significant classification programs completed their first review in July 2012 and provided summaries of those reviews to the Director of the ISSO. Overall, the 2012 reviews showed that Federal agencies were streamlining their classification guidance and more clearly identifying categories of what can be released and what needs to remain classified.

[12] The SAO is the official designated by the agency head under Executive Order 13526, section 5.4(d), to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

The DoJ OIG determined that some agency SCGs did not provide adequate instruction on when and at what level to classify information. In general, all SCGs in use at the agency met the minimum requirements, including, but not limited to, identifying the types and specific topics of information deemed classified and identifying the reasons for classifying the information, the level at which the information should be classified, and the duration of the classification. However, the OIG determined that the creation of SCGs was not sufficiently coordinated, and that some SCGs could have provided additional clarification on specific details to ensure that derivative classifiers make informed and accurate classification decisions.

The EPA OIG determined that its agency had no official SCGs, as required by Executive Order 13526, section 2.2(d), even though the agency had made original classification determinations.[13] According to the team leader for the CNSI program, the agency had not established SCGs because it had classified only a few documents. Furthermore, agency policy required that an SCG be developed for each system, plan, program, or project that involved classified information. Therefore, the OIG determined that the lack of SCGs was a material internal control weakness in the agency's CNSI program.

The USDA OIG reported that the agency's SCG gave a range of years (5 to 25), instead of a specific date or event for declassification. Agency staff told the OIG that subject matter experts set the duration of classification based on their subject matter expertise. However, 32 CFR section 2001.22(a) states that information classified derivatively on the basis of an SCG must carry forward the markings taken from the instructions in the appropriate SCG.

2016

In 2016, three agencies reported on findings from SCG reviews, one agency found no discrepancies, while 10 agencies did not address this area. The DoD OIG reported that the DoD was in the process of implementing 2013 recommendations. The DoD was revising its policy to require that SCGs be submitted and reviewed in a timely manner, forwarded with completed documentation, and signed by the appropriate OCA to ensure accountability. In addition, reminders would be sent to organizations as SCGs near their five-year required reviews.

[13] An original classification determination is an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

The EPA OIG reported that corrective actions to address 2013 recommendations had been addressed, except for two related to SCGs. The OIG found that the EPA still had not ensured the preparation, review, approval, and distribution of SCGs.

Conclusion

In 2013, 9 of the 13 OIGs reported that OCAs in their agencies were appropriately designated, one OIG found discrepancies, and three OIGs did not address the issue. Also, 8 of the 13 OIGs found discrepancies with aspects of OCA program knowledge, three OIGs found no discrepancies, and the remaining two OIGs did not address the issue.

A sampling of 472 SCGs reviewed by 5 of the 13 OIGs in 2013 and 3 of the 13 OIGs in 2016 found that most SCGs in 4 of the 5 agencies were missing required elements needed for derivative classifiers to make proper derivative classification decisions. The five OIGs determined that guidance was needed to address missing or inaccurate declassification dates, proper use of dissemination control and handling markings, and the proper process and points of contact for challenging classification. This information is essential to derivative classifiers who challenge classification determinations. In addition, information sharing can be hindered if information is misclassified and allowed to remain unchallenged.

Without adequate SCGs, agency staff and other users of classified information may not be uniformly and consistently identifying and classifying documents. Ultimately, information that should be protected could be unintentionally released, resulting in harm to national security, and other information that should be released could be inappropriately classified. Clear classification guidance from OCAs can support more accurate derivative classification determinations.

SUMMARY OF FINDINGS

Derivative Classification

In 2013, all 13 OIGs' reports identified discrepancies in derivative classification. The OIGs attributed the discrepancies to problems with document reviews, derivative classifier input, and CMT[14] shortfalls that adversely affected derivative classification. In 2016, 11 of the 13 OIGs identified discrepancies. The OIGs determined that the derivative classification problems were related to inconsistent standards within agencies, disparate marking methods employed by derivative classifiers, and inaccurate and outdated agency CMTs that supported the classification marking process.

Derivative Classification

This section highlights findings from OIG reports in 2013 and 2016 specific to derivative classification knowledge and guidance. The OIG reports addressed three common themes: derivative classifier input, document reviews, and the CMT.

Derivative classifiers are employees who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by an SCG in accordance with Executive Order 13526, section 2.1, and 32 CFR section 2001.22. OIGs interviewed derivative classifiers to assess their knowledge of derivative classification principles and procedures. This section highlights OIG findings from interviews of derivative classifiers, reviews of derivatively classified documents, and reviews of agency CMTs. The problems identified by OIG reviews of the agencies' derivative classification programs are summarized in the following table.

[14] The CMT is an automated tool that allows the user to apply correctly formatted classification markings to electronic documents. Based on classification criteria the user selects, the CMT automatically generates portion marks, a classification banner (header and footer) and block. The CMT also allows the user to validate the portion marks against the banner, ensuring marking consistency and more effective protection of Classified National Security Information.

Table 2. Agency OIG Reviews of Derivative Classification

Dept./ Agency	Identified Issue(s)		Derivative Classifiers Input		Document Reviews		Classification Management Tools	
	2013	2016	2013	2016	2013	2016	2013	2016
DoD	X	X	X	X	X	X	X	X
DHS	X	X	X	X	X	X	X	X
DOC	X	X	N/A	N/A	X	X	N/A	N/A
DOT	X	X	X	X	X	X	N/A	N/A
Energy	X	X	X	X	X	X	X	X
EPA	X	N/A	N/A	N/A	X	N/A	N/A	N/A
HHS	X	X	X	N/A	X	X	N/A	N/A
Justice	X	X	X	N/A	X	N/A	X	X
NRC	X	X	X	X	X	X	N/A	N/A
State	X	X	X	N/A	X	X	X	X
Treasury	X	X	N/A	X	X	X	N/A	N/A
USAID	X	X	X	X	X	X	X	X
USDA	X	N/A	X	N/A	X	N/A	N/A	N/A

Input from Derivative Classifiers

The participating OIGs interviewed or surveyed agency staffs and reviewed comments from derivative classifiers to assess their knowledge of the classification process and the appropriateness of derivative classification actions. The OIGs also asked whether derivative classifiers had encountered issues with the classification of similar information at various levels, inaccurate portion markings, conflicting guidance, and the constraints that control markings might place on information sharing.

2013

In 2013, 10 of the 13 OIGs identified issues during their interviews or surveys of 542 derivative classifiers. The remaining three OIGs did not address this area.

Derivative classifiers expressed concerns about conflicting standards and inconsistent markings encountered when classifying information based on previously classified documents. This was particularly evident with e-mails. Derivative classifiers use various methods to resolve classification discrepancies, which can adversely affect

the sharing of classified information with key stakeholders and individuals with an identified need to know. To accurately address conflicts and inconsistencies, derivative classifiers should refer to an updated and approved agency SCG.

SCG Use

The DHS OIG found that 95 of 100 derivative classifiers surveyed possessed an overall understanding of the derivative classification process and an ability to derivatively classify information properly. However, the OIG found that 15 of 75 interviewed personnel had not used or even seen an SCG. Derivative classifiers believed that senior management direction and policies were sufficient to support the creation, protection, and dissemination of classified documents. The personnel stated that they had seen improvement in security practices, as well as in classifying and marking documents, since 2011.

The Department of Energy (DoE) OIG found that derivative classifiers were not familiar with the processes for directing classification challenges to external entities. They were aware, however, of their responsibility to seek clarification from internal sources.

The DoJ OIG found that agency classifiers did not use SCGs when making derivative classification decisions. In addition, agency personnel stated that they were more likely to "err on the side of caution" when it came to classifying information. When there was any doubt about whether information should be classified, various officials in several components at this agency stated, they would most likely classify the information to avoid the risk of accidently releasing Classified National Security Information. The surveyed personnel did not express significant concern for possibly over-classifying information. Instead, some noted the lack of consequences for taking that action.

Improper Classification Markings and Policy

The DoD OIG found that 60 percent of 129 derivative classifiers surveyed encountered similar information in documents classified at different levels. Among those respondents, 68 percent identified concerns with the inconsistent application of portion markings in classified documents, and 27 percent expressed concerns about the use of dissemination controls (for example, "no foreign dissemination"), which could unnecessarily restrict information sharing. Furthermore, 18 percent of the respondents indicated that when they tried to resolve classification inconsistencies, the guidance was neither clear nor consistent. Respondents also cited conflicting guidance regarding dissemination control markings.

The Department of Transportation (DoT) OIG, after finding a high incidence of improperly marked briefing materials, interviewed agency derivative classifiers, who stated that they did not properly mark derivative products because they did not intend to release the documents outside of the agency. The personnel also stated that some documents, such as briefings and threat analyses, were originally considered working papers—to be destroyed within 180 days—but that operational issues required the documents to be kept for a longer period. The OIG reported that the agency had revised internal guidance to address this issue.

2016

In 2016, 7 of the 13 OIGs identified issues during interviews or surveys of 2,200 derivative classifiers.

SCG Use

The DoD OIG recommended that policy be revised to incorporate template language for SCGs. The OIG found that the language had been incorporated in an ongoing policy revision; however, the policy was undergoing final review in 2016.

The USAID OIG found that an SCG issued in May 2015 did not list a point of contact for questions or provide guidance to users as a mechanism to report needed changes, as the Code of Federal Regulations requires.

Improper Classification Markings and Policy

The USAID OIG found that although policy for classification markings was clear, derivatively classified documents and e-mails were not properly marked. The OIG's assessment found that noncompliance spanned every category reviewed, with the "portion marking" category having an 86 percent error rate.

The Department of the Treasury (Treasury) OIG reviewed 108 derivative classification decisions (71 e-mails and 37 non-e-mails) selected from the population of 147,785 derivative classification decisions reported in fiscal year 2015. The review disclosed that 97 of the decisions (90 percent of the sample) contained one or more errors. Errors related to the classification authority block, portion markings, dissemination control markings, and e-mail responses.

Document Reviews

In their 2013 and 2016 reports, OIGs reviewed 3,797 documents and e-mails. These document reviews identified inconsistent standards and markings for derivatively classified products, which were particularly evident in e-mails.

2013

In 2013, all 13 OIGs identified issues during reviews of derivatively classified documents.

The DoD OIG reviewed 220 classified documents for consistency in portion markings, dissemination controls, classification authorities, and declassification guidance. Seventy percent of those documents had classification discrepancies. For example, 23 documents (approximately 10 percent) were misclassified or over-classified. Additional errors were found in the classification block, including improper citation to Executive Order 12958, which was superseded by Executive Order 13526.[15] Most notably, 100 percent of reviewed e-mails contained errors in marking or classification.

The DoE OIG reviewed 231 documents and e-mails and found that 65 percent of reviewed documents had errors that could hinder efforts to protect CNSI against loss or unauthorized disclosure and could impede information sharing. These errors included over- or under-classification, improper annotations regarding the duration and source of protection, and missing information on the origin and level of protection.

The HHS OIG reported finding few errors during a review of derivatively classified documents. According to the OIG's report, 27 of 30 derivatively classified documents sampled for review met all established requirements. The three documents with errors lacked the required paragraph markings, but met all other Federal requirements. The low error rate was notable because it was the exception among reporting OIGs.

The Treasury OIG reported that incomplete markings it found during component reviews may have occurred because employees: (1) did not take the time to properly mark the e-mails, (2) did not believe that the markings were important, or (3) unintentionally replied to or forwarded e-mails without realizing that such actions were classification decisions. Following the review, the agency created a handout to remind employees that classification markings must appear on all e-mails.

[15] 32 CFR section 2001.21 requires that the classification block contain information on the classification authority, agency and office of origin, reason for classification, and declassification instructions.

OIGs in some agencies such as DoT and EPA with smaller classified holdings also found that a high percentage of documents contained errors, ranging from 72 percent of documents reviewed to 100 percent.

2016

In 2016, 10 of the 13 OIGs again identified issues during reviews of derivatively classified documents.

The DoD OIG reported a decrease in the percentage of documents with errors, from 70 percent in 2013 to 63 percent in 2016, attributing the improvement to enhanced policy and training efforts and the use of CMT.

The DoE OIG reviewed 232 documents and found no under-classification issues, but found 17 documents that were over-classified and 153 marking errors.

The HHS OIG, after finding few documents with errors in 2013, reported in 2016 a 28 percent error rate specifically related to the failure to include the position of the person who derivatively classified the document.

The DoT OIG estimated that 7.5 percent of documents at one component and 3.5 percent of documents at another component reviewed were over-classified. The OIG reported improvements in the manner in which derivatively classified documents complied with ISOO control-marking requirements. The OIG found 9 instances of over-classification or under-classification and marking errors in 47 of 70 sampled documents, or 67 percent of the documents reviewed. The OIG reported that this was a slight improvement over the 72 percent of documents with errors that it reported in 2013.

Classification Management Tool

A CMT should allow a user to apply correctly formatted classification markings to electronic documents automatically. Based on classification criteria the user selects, the CMT automatically generates portion markings, a classification banner (header and footer), and a classification authority block to cover original and derivative information. The CMT also allows the user to validate the portion markings against the banner, helping to ensure consistent markings and protection of national security information.

2013

In 2013, 6 of the 13 OIGs identified issues during their reviews of CMTs. The remaining seven OIGs did not address this area.

The six OIGs that addressed CMTs in their 2013 reports identified ways in which the CMT hindered accurate derivative classification. The OIGs identified the following key issues: training and oversight—a need for better training for derivative classifiers on the use of the CMT; ensuring that the CMT was aligned with Executive Order 13526 and agency policy requirements; CMT deployment—ensuring that all derivative classifiers had a CMT; outdated CMTs—ensuring that derivative classifiers had the most current CMT; and user-friendly CMTs—ensuring that users could easily and effectively use the CMT.

For example, the DHS OIG found that not all of its agency components were using CMTs, and that CMTs being used had not been updated to reflect changes resulting from the publication of Executive Order 13526.

The DoD OIG found that 100 percent of e-mails reviewed that were marked using a CMT contained errors in marking or classification. Of particular concern was the amount of misclassification in routine information and e-mails on classified information systems. The OIG concluded that this misclassification often resulted from default e-mail marking tool settings that allowed the user to accept the default without further consideration of whether other markings were required by the e-mail's content.

The DoE OIG found that a CMT embedded in a classified e-mail system automatically marked e-mails as Secret//Restricted Data, the highest level of protection authorized for that system, regardless of content.

The DoS OIG found that the CMT application contributed to the discrepancies found in document markings because it did not allow classifiers for both derivative and original classifications to include their names and positions, which is contrary to the guidance in Executive Order 13526. In addition, only 54 percent of the agency components (185 of 343) were using the CMT.

The DoJ OIG found that the CMT was available only to two components that were part of the Intelligence Community. At the time, the OIG did not address CMTs in depth because the agency had not deployed a CMT for use by all derivative classifiers.

2016

In 2016, 6 of the 13 OIGs identified issues during reviews of CMTs. The remaining seven OIGs did not address this area.

The key issues of training and oversight, lack of CMT deployment, outdated CMTs, and lack of user-friendly CMTs remained. The OIGs, however, found progress in these four areas.

For example, the DHS OIG found that in 2014, the agency deployed a new CMT to help users mark classified documents and e-mails. In 2016, the OIG reviewed 269 documents and found 48 classification marking errors, an error rate similar to the 59 classification marking errors identified during a review of 372 documents in 2013. The OIG concluded that training, as well as using the CMT when creating classified documents, would help derivative classifiers identify and correct many of the errors.

The DoD OIG noted improvements in the marking of documents, with an error rate of 63 percent in 2016 compared with 70 percent in 2013. The OIG also reported a decrease in the error rate for reviewed e-mails from 100 percent to 85 percent, which the OIG concluded could be attributed to training and the use of CMTs. Of 106 security managers surveyed, 46 (43 percent) identified the presence of e-mail CMTs within their agency.

The DoJ OIG determined that the agency conducted a feasibility study related to CMT use early in FY 2014. The agency established a working group to develop guidance on the use of a CMT, and to identify requirements for implementing it on classified terminals. The system became operational late in FY 2015. The OIG assessed user response and feedback to the new system. The OIG reported that users initially had difficulty with the system due, in part, to a lack of knowledge on classification marking. However, the OIG determined that use of the CMT enhanced the agency's classification management program and increased awareness of classification procedures.

The DoS OIG reported problems with an updated version of the agency CMT. The updated CMT allowed derivative classifiers to classify information as an original classifier when the user did not have that authority. As a result, the OIG recommended that the agency implement a control on the system to allow only individuals with OCA the ability to classify information in that manner.

The USAID OIG found that although derivative classifiers requested and were provided training on the CMT, a review of classification markings identified numerous errors. The OIG determined that the numerous errors indicated that the training provided had not been effective at improving compliance.

Conclusion

Reporting OIGs identified human error by derivative classifiers; lack of management guidance on originally classified documents, policies, and SCGs; and outdated or inaccurate CMTs as common issues of concern. The OIGs also identified training (which is discussed in a separate section of this report) as necessary to correct errors among derivative classifiers. The OIGs also recommended updating policy and CMTs to align with Executive Order 13526 to correct lapses in classification management and automation. While still identifying problems in 2016, most OIGs also noted improvements in the application of derivative classification.

SUMMARY OF FINDINGS

Program Management

In 2013, 5 of the 13 OIGs found that their agencies had not adopted applicable classification policies, procedures, rules, and regulations. In 2016, 3 of the 13 OIGs found that their agencies still had not done so.

In 2013, 11 of the 13 OIGs found that their agencies did not fully follow or effectively administer guidance as required. In 2016, 7 of the 13 OIGs determined that their agencies still had not done so.

In 2013, 5 of the 13 OIGs found instances of over-classification. In 2016, 3 of the 13 OIGs still found instances of over-classification.

In 2013 and 2016, only one OIG each year found that its agency had a strong CNSI program. The other 12 OIGs identified challenges that included:

- ineffective oversight of classification activities,
- inaccurate reporting to the ISOO,
- inadequate and inconsistent use of SCGs,
- inadequate and outdated policy,
- insufficient resources,
- inadequate records management,
- inadequate training,
- inadequate implementation of classification and control marking guidance,
- outdated CMTs,
- OCA reductions, and
- lack of a critical element for security in the performance evaluations of those employees whose duties require significant handling of classified information.

This section highlights issues identified by the OIGs related to the management of their agencies' Classified National Security Information (CNSI) program. Program management, which refers to the responsibilities of agencies carrying out the CNSI program under Executive Order 13526, includes a personal commitment to the program demonstrated by the agency head, dedication of necessary resources to

ensure effective implementation of the program, and appointment of a Senior Agency Official (SAO) to administer the program. The problems identified in the OIGs' reviews of their agencies' program management are summarized in the following table.

Table 3. CNSI Program Management

Dept./ Agency	Identified Issue(s)		Adopted Applicable Policies		Followed and Administered Guidance		Over-Classification Found	
	2013	2016	2013	2016	2013	2016	2013	2016
DoD	X	X	✓	✓	X	X	X	N/A
DHS	✓	N/A	✓	N/A	✓	N/A	N/A	N/A
DOC	X	N/A	✓	N/A	X	N/A	N/A	N/A
DOT	X	X	X	X	X	X	N/A	X
Energy	X	X	✓	✓	X	X	X	X
EPA	X	N/A	X	N/A	X	N/A	X	N/A
HHS	X	X	✓	N/A	✓	N/A	N/A	N/A
Justice	X	X	✓	✓	X	✓	X	X
NRC	X	✓	X	✓	X	✓	N/A	N/A
State	X	X	✓	✓	X	X	X	N/A
Treasury	X	X	✓	✓	X	X	N/A	N/A
USAID	X	X	X	X	X	X	✓	N/A
USDA	X	X	X	X	X	X	✓	✓

Agencies are required to issue policy to carry out their CNSI programs in accordance with Executive Order 13526 and 32 CFR Part 2001. To evaluate the CNSI programs, OIGs also used an "Agency Regulation Implementing Assessment Tool," which focused on:

- original classification authority,
- original classification, including control markings,
- derivative classification, including control markings,
- general program management responsibilities,
- security self-inspections,
- security reporting,

- security education and training, and
- Intelligence Community cross-cutting issues, as applicable (see "Intelligence Community Reporting" in Appendix C).

As previously discussed, each OIG of an agency with an officer or employee who is authorized to make original classifications assessed whether applicable classification policies, procedures, rules, or regulations were adopted, followed, and effectively administered. In addition, the OIGs identified policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material.

General Classified National Security Information Program Management and Policy Compliance

Each OIG reviewed the CNSI program and the use of dissemination control markings to determine whether the agency designated an SAO to direct and administer the program, dedicated necessary resources for effective implementation of the program, and designed and maintained records systems to optimize appropriate sharing and safeguarding of classified information.

The Information Security Oversight Office (ISOO) develops, coordinates, and issues implementing directives and instructions regarding Executive Order 13526. The ISOO provided an "Agency Regulation Implementing Assessment Tool" to assist OIGs in determining whether applicable classification policies, procedures, rules, and regulations had been adopted in accordance with Executive Order 13526 and 32 CFR Part 2001.[16]

As with agencies, the ISOO provided the assessment tool to the OIGs to use as a checklist to assess agency policy conformity with Executive Order 13526 and 32 CFR Part 2001. In some cases, OIGs mapped agency-level policy issuances to Executive Order 13526 and 32 CFR Part 2001 to verify compliance, to assess whether classifiers understood the Executive order and the regulation, and to determine whether decisions on classification and dissemination controls were made correctly.

[16] The "Agency Regulation Implementing Assessment Tool" focuses on eight key areas (original classification authority, general program management responsibilities; classification; declassification; safeguarding; self-inspections; security education and training; reporting and definitions).

The term "over-classification" is not defined in Executive Order 13526 and 32 CFR Part 2001. Executive Order 13526 defines "classification" and "declassification," but not this term. In this summary report, we have used a working definition of "over-classification," which ISOO supplied: the designation of information as classified, when the information does not meet one or more of the standards for classification under section 1.1 of Executive Order 13526.[17]

In 2013, all 13 OIGs provided information on general classification program management and policy compliance. In 2016, 10 of the 13 OIGs provided information on general classification program management and policy compliance. The following examples highlight issues they identified related to CNSI program management.

Adopted Applicable Policies

In 2013, 5 of the 13 OIGs found that their agencies had not adopted applicable classification policies, procedures, rules, and regulations. In 2016, 3 of the 13 OIGs found that their agencies still had not done so.

2013

Five of the 13 OIGs found that their agencies had not adopted applicable classification policies, procedures, rules, and regulations. Eight of the 13 OIGs determined that policies and procedures mapped to Executive Order 13526 and 32 CFR Part 2001 were adopted by the agency.

For example, the DoT OIG noted that policies and procedures were not effective and did not fully comply with Executive Order 13526 and 32 CFR Part 2001.

The EPA OIG determined that policies and the basic guidance documented for the agency CNSI program did not reflect current Government-wide requirements, and that the basic guidance document was not an agency-wide directive even though it affected the entire agency.

The Nuclear Regulatory Commission (NRC) OIG determined that some agency policies were not updated in a timely manner to correspond with certain ongoing classification practices.

[17] Executive Order 13526, section 1.1 (Classification Standards), states that information may be originally classified only if an OCA is classifying the information; the information is owned by, produced by or for, or is under the control of the United States Government; the information falls within one or more of the categories of information listed in Executive Order 13526, section 1.4 (Classification Categories); and the OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage. If there is significant doubt about the need to classify information, it shall not be classified.

The USAID OIG determined that the agency classification policy did not meet the requirements set forth in Executive Order 13526 and 32 CFR Part 2001.

The USDA OIG found that the agency lacked proper classification management guidance and a records management system to identify documents that must be declassified or reviewed for continued national security.

However, the DoD, DHS, DoC, DoE, DoJ, DoS, HHS, and Treasury OIGs found that their agencies had adopted applicable classification policies, procedures, rules, and regulations prescribed by Executive Order 13526 and 32 CFR Part 2001.

2016

In 2016, 3 of the 13 OIGs found that their agencies still had not adopted applicable policies. Five OIGs still determined that policies and procedures mapped to Executive Order 13526 and 32 CFR Part 2001 were adopted by the agency. One OIG noted improvement, and four OIGs did not address the issue.

For example, the DoT improved its compliance with Federal requirements for classification since the OIG's 2013 review through more comprehensive programs for employee training and agency self-inspections. However, some weaknesses persisted with two components. Of particular concern was one component's outdated policy on safeguarding CNSI—an issue identified in 2013. The component's reliance on a policy that had not been updated since 2006 contributed to instances of noncompliance with more recent Federal requirements, such as derivative classifier identity.

The USAID OIG found that the agency's classification policy did not meet the requirements set forth in Executive Order 13526, and that the central security office had not effectively administered the agency's CNSI program. The OIG found persistent and systemic noncompliance related to program management, security education and training, self-inspections, the issuance of an agency SCG, reporting of program activities and results to the ISOO, and classification markings.

The USDA OIG noted that the agency's central security office did not have an internal control structure sufficient to minimize the risk of over-classifying or improperly releasing national security information, despite the agency's agreement to take appropriate actions toward that goal in response to the OIG's 2013 audit of CNSI. The 2013 audit made 17 recommendations to improve the agency's classification management program. The OIG determined that the agency fully implemented 2 recommendations and had not timely implemented 11 recommendations related

to policy revisions and a reduction in OCA authority. However, the OIG found that although corrective actions were implemented for 6 recommendations, weaknesses still existed in 4 of those recommendations.

However, the DoD, DoE, DoJ, DoS, NRC, and Treasury OIGs found that their agencies had still adopted applicable classification policies, procedures, rules, and regulations prescribed by Executive Order 13526 and 32 CFR Part 2001.

Followed and Administered Guidance

In 2013, 11 of the 13 OIGs determined that their agencies did not fully follow or administer the policies. In 2016, 7 of the 13 OIGs determined that their agencies did not fully follow or administer the policies.

2013

In 2013, 11 of the 13 OIGs determined that their agencies did not fully follow or administer the policies.

For example, the DoD OIG found that although the agency had adopted applicable classification policies, procedures, rules, and regulations, that they had not been followed or effectively administered in some circumstances. The OIG also concluded that some policies, procedures, rules, regulations, or management practices may be contributing to persistent misclassification of material. The OIG found several instances in which the inaccurate use of dissemination control and handling markings could unnecessarily restrict information sharing. Many of the issues the OIG found were similarly reflected in agency self-assessments and FCGR results. The most common discrepancy found at the DoD was incorrect marking of documents. Also, many interviewees commented on the lack of availability and robustness of training designed for employees charged with original and derivative classification duties.

The DoJ OIG found that the agency had developed classification program oversight and review processes, but had not successfully implemented those processes because of insufficient resources, deficient oversight, and inadequate assistance from agency components. The OIG also found that many of the classification deficiencies it identified were attributable to various factors associated with the agency's implementation of its classification management program. These factors included deficiencies in the agency's implementation of classification and control marking guidance, inadequate and inconsistent use of SCGs, a lack of automated tools capable of improving classification processes, deficiencies in the systems

infrastructure used to process and store classified information, and weaknesses in the agency's security education and training programs. Also, the central security office, responsible for ensuring that policies and procedures comply with all regulations and Federal requirements, did not adequately address the following requirements of Executive Order 13526:

1. prohibition of retribution for challenging the classification of information;
2. a process of transferring ownership of classified information with a transfer of functions;
3. incorporation of classification management into performance plans and evaluations for OCA officials, derivative classifiers, and security programs officials; and,
4. publication of the updated Mandatory Declassification Review process in the Federal Register.

The DoS OIG determined that although the agency generally had adopted classification policies, procedures, rules, and regulations prescribed by Executive Order 13526, two components had not effectively followed all of these rules. The OIG recommended updating or amending policy to reflect that Executive Order 13526 requires classification training; updating the CMT application to facilitate compliance with classification standards; and implementing a methodology to select a representative sample of classified documents for the annual self-inspection, along with a process to validate SF 311 submissions.

The DoT OIG noted that policies and procedures were not effective and did not fully comply with Executive Order 13526 and 32 CFR Part 2001. Specifically, the DoT self-inspection program did not provide adequate coverage of either documents or physical locations; many documents were not properly marked; and the statistics reported to the ISOO contained inconsistencies. Furthermore, a component's policy had not been updated to comply with Executive Order 13526. For example, the existing policy did not contain provisions related to compliance with ancillary marking requirements of derivative classifier identity and declassification date.

The EPA OIG determined that policies and the basic guidance documented for the agency CNSI program did not reflect current Government-wide requirements, and that the basic guidance document was not an agency-wide directive even though it affected the entire agency. The guidance document needed to be updated to incorporate

recent changes in the Government-wide guidance. For example, the document cited Executive Order 12958, "Classified National Security Information," April 1995, as amended; however, that order was superseded by Executive Order 13526 in December 2009.

The NRC OIG determined that some agency policies were not updated in a timely manner to correspond with certain ongoing classification practices. Specifically, although procedures were drafted relative to controls over a particular classified program, those procedures had not been finalized and added to policy. Examples of issues that needed updating included:

- Federal policy references (for example, Executive orders),
- classification categories and declassification exemptions,
- the Third Agency Rule,[18]
- classifier training requirements,
- a secure system for submitting allegations and complaints about misclassification within the agency, and
- specific requirements for reporting to the ISOO.

The USAID OIG determined that not only did the agency's classification policy not meet the requirements set forth in Executive Order 13526, the Office of Security had not effectively administered the agency's CNSI program. The OIG found persistent and systemic noncompliance related to program management, security education and training, self-inspections, the issuance of an agency SCG, classification markings, and program activities reported to the ISOO.

The USDA OIG found that its agency lacked proper classification management guidance and a records management system to identify documents that must be declassified or reviewed for continued national security. The agency's SCG was missing required elements needed for proper derivative classification decisions. Additionally, adequate statistics related to the security classification program were not always obtained and maintained, making it difficult to ensure that components were conducting self-inspections in accordance with regulations and procedures. The OIG noted that agency policies had not been adopted in accordance with Executive Order 13526 and

[18] An agreement among U.S. Government agencies participating in the exchange of intelligence data forbidding one agency to disseminate to another agency information which originated with a third agency—also, the tenet that information usually classified or sensitive, originating in one agency, not be disseminated by another agency to which the information has not been made available without the consent of the originating agency.

32 CFR Part 2001 for many key areas, including general program management and classification challenges. In general, staff members agreed that the agency's policy needed to be updated and explained that they were working on an agency manual.

The OIG also found several weaknesses in the agency's internal management controls of classified material.

- There was no records management system for classified information, and agency policy was outdated.
- The SCG used for making derivative classification decisions was missing required elements.
- Original and derivatively classified documents were incorrectly marked.
- Annual reports were submitted to the ISOO with incorrect information or unsupported information.
- Self-inspection reports were not submitted to the central security office, and ultimately the agency's roll-up report to the ISOO was not supported.
- Training records were not maintained for all agency derivative classifiers.

However, the HHS OIG determined that agency policies for CNSI followed requirements outlined in Executive Order 13526 and 32 CFR Part 2001, annual status reports and self-inspections were accomplished to ensure that CNSI policies were effectively administered, and guidance and training were provided to individuals who access CNSI to ensure that CNSI policies were followed. The OIG also determined that certain agency components developed guidance that further defined policies regarding CNSI for specific programs. A draft policy on interagency information sharing across Federal agencies within the national security community also was developed.

2016

In 2016, 7 of the 13 OIGs determined that their agencies still did not fully follow or administer the policies.

The DoE OIG found that the agency implemented five of seven recommendations, including updating CNSI policies. The agency and a component also implemented training for preparing classified working papers, portion marking e-mails, and addressing classification challenges. In addition, the agency provided guidance regarding derivative classifiers' accountability. The OIG noted that striking a balance between protecting CNSI and sharing information appropriately is difficult even in

optimal circumstances. However, the OIG noted that effective oversight, training, and well-developed guidance for those involved with classifying national security information are imperative if the agency is to be successful in this effort.

The Treasury OIG determined that the agency had put policies and procedures in place to safeguard classified materials, but continued to have difficulty ensuring that these policies and procedures were consistently followed. Findings for the followup evaluation were similar to those identified in the 2013 report. The OIG noted continuing concerns with: (1) classification marking decisions, (2) completing the SF 311, and (3) complying with self-inspection requirements.

Some agency OIGs also reported compliance with existing policies. For example, the DoJ OIG determined that the agency improved its classification management program with updated classification guidance, instruction, and training. Also, as previously mentioned, the agency reduced the number of OCAs from 64 to 46, to ensure that OCA delegations are limited to the minimum number necessary to administer Executive Order 13526.

Over-Classification Found

In 2013, 5 of the 13 OIGs found instances of over-classification. In 2016, 3 of the 13 OIGs still found instances of over-classification.

2013

In 2013, 5 of the 13 OIGs found instances of over-classification, 2 OIGs did not find over-classification, and 6 OIGs did not address over-classification.

For example, the DoE OIG determined that of the 231 documents and emails reviewed, 65 percent had classification marking errors that could adversely affect efforts to protect CNSI against loss or unauthorized disclosure and impede information sharing. These errors included: (1) over- or under-classification; (2) improper annotations regarding duration and source of protection; and, (3) missing information on the origin and level of protection.

The DoD OIG reviewed 220 classified documents for consistency in portion markings, dissemination controls, classification authorities, and declassification guidance and found that 70 percent of the 220 documents reviewed had classification discrepancies. Moreover, 23 documents, or approximately 10 percent, were misclassified or over-classified. A majority of the documents (52 percent) had issues with the classification block to include incorporating new guidance regarding the “classified by” line. Without

the "classified by" information, challenging an incorrect classification decision would be problematic. Other documents still cited Executive Order 12958 for classification authorities and declassification exemptions.

The EPA OIG identified portions of a scientific report that seemed to be over-classified. The report acknowledged there were doubts as to whether the release of some of the report data would constitute a threat to national security, but the information was nonetheless classified. As noted in Executive Order 13526, if there is doubt, information should be unclassified or classified at a lower level. In response to OIG questions, the central security office offered satisfactory explanations for classifying the information and explained the threat that the release of such information would pose.

The DoS OIG reviewed 34 classified documents created in 2011 to assess the agency's compliance with Executive Order 13526's classification standards and found that one of the 34 documents reviewed was over-classified. The over-classification occurred because the document preparer copied the markings and the classification level from the original telegram but the content of the new telegram did not contain any classified information. In addition, the preparer, when interviewed, stated that she had not taken the agency's mandatory training.

The DoJ OIG reviewed a sample of 25 original classification decisions and 116 derivative classification decisions from agency components. The OIGs review identified several discrepancies, including incorrect designations of decisions as "original" classification decisions, information that had been inappropriately identified as classified (over-classification), improper use of a dissemination control, and unmarked or incorrectly marked documents containing CNSI.

The USAID OIG determined that although none of the 21 documents in a representative sample was over-classified, only 5 documents were marked correctly. The agency did not issue an SCG or update parts of the classification policy. Executive Order 13526 requires agencies to develop their own SCGs.

The USDA OIG determined that derivative classifiers did not have adequate information to make a proper and uniform derivative classification decision, which could lead to a misclassification or over-classification of information.

2016

In 2016, 3 of the 13 OIGs still found instances of over-classification, 1 OIG did not find over-classification, and 9 OIGs did not address over-classification.

The DoT OIG determined that unless the agency fully addresses recommendations, the agency risks that documents might not be properly classified or sufficiently protected. The OIG found few instances of over-classification—about 7.5 percent in one component and about 3.5 percent in another component. In preparing documents, both components use ISOO guidance and, aside from these exceptions, conformed to the ISOO's guidance. The OIG did note a practice that, while conforming to ISOO guidance, could result in over-classification of information in derivative documents. The practice involved using sources at different classification levels in one paragraph. As required, the paragraph should be marked for the highest level of information within the paragraph. However, subsequent users may assume that all information is at the same level and apply an incorrect, higher classification level when they extract information from the paragraph. The OIG did not find any instances at DOT when this situation occurred and resulted in over-classification.

The DoJ OIG found that one component may be implementing classification practices that result in the under- or over-classification of information.

The DoE OIG determined that of the 232 documents and e-mail selected for review, none had critical errors (for example, under-classification), 17 had major errors (for example, over-classification), and 153 had marking errors. The major errors included over-classification and incorrect declassification instructions. The marking errors included missing or incomplete portion marking of documents and e-mail and missing or incomplete derivative classifier's agency or organization information. None of the errors we observed would likely result in the inappropriate release of classified information.

Security Education and Training

This section highlights findings from OIG reports in 2013 and 2016 specific to agency security education and training programs. The OIG reports addressed four common themes: original classifier training, derivative classifier training, training policy, and training curriculum.

This section also indicates whether agency polices mandate initial security training, refresher training, specialized training, or training for OCAs and persons who apply derivative classification markings, and whether the policies require suspending original and derivative classification authority if these personnel fail to meet the training requirements.

OIGs interviewed OCAs, derivative classifiers, and agency security and training representatives to determine if employees who create, process, or handle classified information have a satisfactory knowledge and understanding of classification policies and procedures. The intent was also to determine the effectiveness of agency security education and training programs, including the extent to which agencies implemented or developed a security education and training program, in accordance with Executive Order 13526 and 32 CFR sections 2001.70 and 2001.71.

In 2013, 7 of the 13 OIGs identified concerns with OCA training. According to the 2013 reports, most OCAs received training as prescribed; however, curriculum and training updates in policy were still being developed and refined to align with Executive Order 13526 and 32 CFR sections 2001.70 and 2001.71. In 2016, only two OIGs identified concerns with OCA training.

Similarly, in 2013, 9 of the 13 OIGs identified concerns with derivative classifier training. In 2016, only three OIGs identified such concerns.

In 2013 and 2016, OIGs also determined that CMT training could be improved to enhance classification marking in the electronic environment.

None of the OIGs identified an occurrence when its agency suspended original or derivative classification authority for employees failing to meet training requirements. The problems identified by OIG reviews of the agencies' training programs are summarized in the following table.

Table 4. Agency OIG Reviews of Training

Dept./ Agency	Identified Issue(s)		Original Classifiers		Derivative Classifiers		Training and Policy		Curriculum	
	2013	2016	2013	2016	2013	2016	2013	2016	2013	2016
DoD	X	✓	✓	✓	X	✓	✓	✓	✓	✓
DHS	✓	X	✓	N/A	✓	X	✓	N/A	✓	N/A
DOC	X	X	N/A	N/A	X	N/A	X	X	X	N/A
DOT	N/A	✓	N/A	✓	N/A	✓	N/A	✓	N/A	✓
Energy	X	X	✓	✓	✓	✓	✓	✓	X	X
EPA	X	✓	X	N/A	X	N/A	X	✓	N/A	N/A
HHS	X	N/A	✓	N/A	X	N/A	✓	N/A	N/A	N/A
Justice	X	✓	X	✓	X	✓	X	✓	X	✓
NRC	X	✓	X	N/A	✓	N/A	X	N/A	X	✓
State	X	X	X	N/A	X	N/A	X	X	N/A	X
Treasury	X	X	X	X	X	X	X	X	N/A	X
USAID	X	X	X	N/A	X	N/A	N/A	N/A	N/A	X
USDA	X	X	X	X	X	X	X	X	X	X

Original Classifier Training

OCAs are authorized to originally classify information. To ensure that OCAs are aware of their responsibilities and equipped to adequately manage the agency's handling of classified information, they are required to complete training. Executive Order 13526, section 1.3(d), and 32 CFR section 2001.70(c)(3) state that OCAs are required to receive training before classifying original information and then at least once each calendar year thereafter. The annual training must include guidance on proper classification and declassification procedures, with an emphasis on the avoidance of over-classification.

Some OIGs found issues related to the frequency and documentation of training. However, most OIGs determined that OCAs were knowledgeable and capable of executing their mission in accordance with Executive Order 13526.

2013

Of the 13 OIGs, 7 identified issues with OCA training in their 2013 reports. Of the remaining six, four reported no concerns and two did not address the issue.

For example, the DHS OIG determined that all OCAs received annual training as prescribed in Executive Order 13526 and 32 CFR Part 2001. The training covered duties and responsibilities of an OCA, and the proper application of classification markings. OCAs also were made aware that their authority would be suspended if they failed to complete training in a timely manner. The OCAs interviewed were knowledgeable about their duties and responsibilities. They were able to identify and describe the degrees of damage to national security in cases of unauthorized disclosure of Top Secret, Secret, or Confidential information. The OCAs also understood that if they did not carry out their duties as stated in Executive Order 13526 or 32 CFR Part 2001, they could be subjected to sanctions that include reprimand, loss of classification authority, loss or denial of access to classified information, suspension without pay, or removal.

The USAID OIG found that its agency did not have training specifically for OCAs. The agency central security office's training program covered both original and derivative classifiers. Security officials recognized the need for specific OCA training, and the office developed a module to address those requirements during the course of the OIG review.

The USDA OIG determined that the agency offered OCAs only generalized training.[19] The OIG also reported that the central security office did not have documentation confirming that the OCA had completed the training, but according to the agency OCA, initial training was completed, but refresher training was conducted four years later. Furthermore, the OIG found that the agency's central security office did not have documentation confirming that the OCA had completed the required annual training.

[19] 32 CFR section 2001.71(c) states that OCAs must be provided detailed training on proper classification and declassification, with an emphasis on the avoidance of over-classification. At a minimum, the training should cover classification standards, classification levels, classification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

2016

Six OIGs addressed OCA training in their 2016 reports. One OIG found that processes had improved, two OIGs found no discrepancies in both 2013 and 2016, and two OIGs found that issues still remained in 2016. The remaining seven OIGs did not address this area.

The Treasury OIG determined that the 2015 e-mail records of completed training did not support the completion rate reported to the ISOO. Furthermore, the agency reported 100 percent completion for the required OCA training in FY 2014 to the ISOO. However, documents the OIG reviewed disclosed that the central security office did not have OCA training records for 9 of the 13 OCA holders in FY 2014. Because training materials were outdated and documentation of the completion of training was not maintained consistently, the central security office could not verify that all employees received the training required by law.

The DoJ OIG reported that the agency reduced the annual number of original classification decisions to zero since 2012. The central security office attributed these reductions, in part, to efforts to enhance its classification training program. These officials stated that DoJ classifiers were more knowledgeable about the appropriate processes for making original and derivative classification decisions.

Derivative Classifier Training

Once an OCA classifies information, that information may be paraphrased, extracted, or summarized, which is known as a derivative classification decision. A derivative classifier must observe and respect the original classification decision and carry forward to any newly created document the pertinent classification markings from the source document(s) or the SCG. To ensure that derivative classifiers are aware of their responsibilities and equipped to adequately manage the handling of classified information, they are required to complete training. Executive Order 13526, section 2.1(d), and 32 CFR section 2001.70(d) state that derivative classifiers are required to receive training before classifying original information and then at least once each calendar year thereafter. The annual training must include guidance on proper classification and declassification procedures, with an emphasis on the avoidance of over-classification. At a minimum, the training shall cover the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, SCGs, and information sharing.

2013

In 2013, 9 of the 13 OIGs identified concerns with derivative classifier training. Three OIGs reported satisfactory levels of derivative classification training. One OIG did not address this area.

The DoC OIG determined that because employees with derivative classification authority did not receive proper guidance and training on policies and procedures, classified documents, or portions of classified documents, could be improperly released. Without improvements, the OIG noted that weaknesses identified may limit the agency's ability to make informed risk-based decisions that support the protection of classified information.

The DoD OIG determined that a majority of derivative classifiers interviewed received no training on the process for challenging information they believed to be inappropriately classified.

The DoS OIG recommended that the agency's central security office add the course "Classified and Sensitive But Unclassified Information: Identifying and Marking" to the agency's mandatory training list to promote awareness of the training requirement. The OIG also recommended that the central security office amend policy to align with Executive Order 13526 language that requires the suspension of classification authority for those who fail to receive classification training. The OIG also recommended that the central security office, in coordination with one component, immediately implement a process to identify agency classifiers who had not met the training requirement and to take the actions required by the amended policy.

The EPA OIG determined that agency personnel with a security clearance were not completing annual refresher training. Better monitoring was needed to ensure that all agency personnel with clearances complete the required training.

The HHS OIG determined that the agency's CNSI policy did not specify who was responsible for ensuring that classification security officers receive training. The OIG recommended that the central security office revise the policy to clarify the responsibility for ensuring that designated classification security officers receive training regarding the handling and safeguarding of classified information.

The USAID OIG determined that derivative classifiers who need to access the classified information system must undergo training, which consists of the Chief Information Officer's cyber-awareness training and the central security office's training. The OIG spoke with 14 agency employees who regularly use the classified information

system. Some stated that they used the CMT recently for classifying e-mails and added that they would like more guidance on using it. They also gave suggestions, such as providing a tutorial, including the tool in security training, e-mailing a guide to classified information system users, or offering a drop-down menu with options. Chief Information Officer staff stated that the classified information system marking tool was deployed only on updated terminals; consequently, not all employees had seen it. Security officials stated that they would work with the Chief Information Officer to train employees on how to use the tool.

2016

In 2016, seven OIGs reported on derivative classifier training. Three OIGs reported continuing issues. Two OIGs reported improved processes for the training of derivative classifiers. The remaining six OIGs did not address this issue in their 2016 reports.

The DHS OIG found that of 102 CMT users interviewed, only 9 stated that they received CMT training. Other users stated that they did not receive training, did not know how to get access to the training, or learned CMT with help from security managers or more experienced users. Without training, some users lacked familiarity with the CMT, which decreased the efficiency of e-mail dissemination.

The Treasury OIG found that Treasury was revising its training program to include reminding derivative classifiers of the obligation to properly mark and safeguard classified information. The central security office was developing a security training campaign to include training on derivative classification decisions and portion markings.

The USDA OIG found that the central security office was still developing training materials although it had estimated that the materials would be completed by September 30, 2014. In 2016, the OIG reviewed the most current versions and concluded that the training material still did not cover all required topics.

The DoD OIG previously recommended greater outreach to inform the security community of training resources. In the 2016 review, the OIG identified headquarters and field-level collaborative efforts that improved training and the marking of classified information. Moreover, the OIG found greater department-level participation in agency security forums and the inclusion of security training links on department-level websites.

The DoJ OIG found that the agency's central security office designated a classification management official to conduct classification marking training sessions and resolve any classification questions related to the use of the CMT. In addition, the central security office deployed additional CMT-specific training seminars and coordinated with the Office of the Chief Information Officer to develop a help desk to assist end users in troubleshooting any CMT software problems.

Training, Education, and Policy

Executive Order 13526, section 2.1, and 32 CFR section 2001.70 state that each agency shall establish and maintain a formal security education and training program which provides for initial training, refresher training, specialized training, and termination briefings. Agency officials responsible for the security education and training programs should determine the specific training to be provided according to the agency's program and policy needs.

2013

In 2013, 7 of the 13 OIGs identified concerns with policy related to training and education. Four OIGs did not identify any concerns, while two did not address this area.

For example, the DHS OIG did not identify any issues and reported that the agency was working to create standardized training across components, incorporating the essential elements for establishing a formal security education and training program for cleared individuals.

The DoJ OIG determined that the agency did not have an explanation of its classification challenge process, which entitles authorized holders of information to challenge the classification status of information when the holder, in good faith, believes that the information is improperly classified. Another aspect of classification management that was missing from the agency's training programs was instruction about what personnel should do when a source document either is not marked or is marked inappropriately. The OIG found documents that agency officials knew were not marked properly, but these officials stated that they did not know how to handle improperly marked source documents. The OIG also determined that many of the classification and marking issues identified throughout the review were attributable to inadequate training. Specifically, individuals responsible for the classification decisions and application of appropriate markings were not aware of the requirements because the available training did not provide personnel with the comprehensive knowledge

of classification policies, procedures, and requirements needed to operate an effective classification management system. According to central security office officials at the agency, resource constraints hindered their ability to operate a robust security education and awareness training program.

The USDA OIG determined that classification management training content and documentation needed improvement, particularly in providing required information to individuals with security clearances. As a result, there was a greater potential for over-classifying or improperly releasing CNSI.

2016

In 2016, two of the OIGs that identified issues with training and education policy in their 2013 reports noted that the issues were resolved. Four OIGs determined that training and education policy issues remained. Two OIGs found no discrepancies in both 2013 and 2016. Four OIGs did not address this area in their 2016 reports or determined that there were still no issues.

In 2013, the DoD OIG recommended that DoD enhance its outreach to the security community to expand awareness of its central security training office. The central security training office subsequently increased delivery methods for security training courses and broadened its outreach efforts, with the goal of improving timeliness of training provided to original and derivative classifiers. The central security training office also implemented additional course offerings that are tailored to original and derivative classifiers.

With regard to the continuing concerns, the DoS OIG determined that most of the agency's security-cleared employees had not taken the training required by Executive Order 13526. Based on training records obtained from one component, the OIG found that less than 14 percent of security-cleared employees had completed the required training within the timeframe considered in the review. Moreover, only 20 percent had completed the training even one time since the outset of the training program. Furthermore, the agency had not implemented the sanction provision that suspends an individual's classification authority until training is completed. These conditions occurred in part because the central security office had not provided adequate guidance to the agency's components specifying how the process for suspending classification authority should work. When employees and contractors

are unaware of classification standards and no mechanism is in place to enforce training requirements, there is an increased risk that information could be incorrectly marked, misclassified, or improperly restricted or disseminated.

The USDA OIG determined that the agency's training program lacked key information and was not in accordance with ISOO regulations or Executive Order 13526. This increased the risk that individuals creating or handling classified information had not been adequately trained to do so, which could result in over-classification, misclassification, or improper release of national security information. The OIG recommended that the central security office develop, complete, and record computer-based training that meets all requirements.

Curriculum

To facilitate training, agencies develop courses of instruction for employees based on Executive Order 13526, section 2.1, and 32 CFR section 2001.70(c). Security education and training should be tailored to meet the specific needs of the agency's security program and the specific roles employees are expected to play in that program. The agency official(s) responsible for the program shall determine the means and methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, online presentations, and other media and methods.

2013

In 2013, 5 of the 13 OIGs identified issues related to security training curriculum. Two OIGs did not identify concerns, and the remaining six did not address this area.

For example, the DHS OIG determined that the agency created, implemented, and conducted adequate original and derivative classification training that was up to date and in compliance with the requirements of Executive Order 13526 and 32 CFR Part 2001. During compliance reviews, the ISOO commended the training management staff for its successful work in conducting and implementing training.

The DoD OIG found that overall, security training and education were effective; however, many interviewees said security education and training were challenging for a number of reasons, including availability, course content, and delivery. Components varied their training programs based on their operating tempo, their need to tailor their training, and their ability to deliver training to their personnel. Although the agency had a robust training component that offered courses that met policy

requirements and could be delivered in various ways, personnel were unaware of both the training component and its associated courses. Without additional outreach to improve awareness of security training and education, agency personnel could be unaware of all available courses.

The DoE OIG found that at the agency headquarters, derivative classifiers were not required to complete derivative classifier training covering the topic of marking classified working papers.

The DoJ OIG found that the DoJ developed security training for original and derivative classifiers. Some delivery methods included self-learning, instructor-led, and electronic training sessions. These training methods did not address all aspects of security and classification requirements, including classification management. An agency OCA stated that the absence of interactive training courses impeded the ability to ask questions.

The USDA OIG found that where training existed, information did not always reflect current requirements. The OIG determined that the agency's program was not aligned with ISOO and Executive Order 13526 requirements. Specifically, training did not cover:

- avoidance of over-classification,
- prohibitions and limitations on classification,
- classification challenges, or
- information sharing.

As a result, the OIG determined, the employees who took the training were not properly trained in all aspects of derivative classification.

2016

In 2016, five OIGs identified issues related to security training curriculum. Four OIGs did not identify concerns, and the remaining four did not address this area.

In 2016, the USAID OIG's review of agency compliance with 32 CFR sections 2001.70 and 2001.71 disclosed that the central security office's training presentations and briefings did not fully comply with the requirements of 32 CFR section 2001.71. Specifically:

- the written training presentation for the initial security briefing did not cover criminal, civil, or administrative sanctions;

- the written training presentation for original classification authorities did not cover the duration of classification, identification and markings, classification prohibitions and limitations, use of the SCG, or information sharing;
- the written training presentation for the annual security refresher training did not cover classification prohibitions and limitations, sanctions, or use of the SCGs;
- termination briefings did not cover sanctions for noncompliance or employees' obligation to return all classified documents and materials in their possession; and
- the central security office did not use standard training materials, permitting instructors to make presentations with differing content.

The USDA OIG found that the central security office was still developing training materials. The OIG reviewed the most current revisions and concluded that the training slides still did not cover all required topics. For example, the OIG noted that the executive briefing slides for OCAs did not cover duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, or information sharing.

The DoJ OIG found that the central security office improved its training platform with updated material to provide guidance on how to apply classification markings in accordance with SCGs and information on how to access additional classification resources. The central security office deployed the updated training to component personnel who are authorized access to classified information, including OCAs, declassification authorities, security managers, security specialists, and all other personnel whose duties involved the creation or handling of classified information. The OIG reviewed the updated training materials and found that the materials provided guidance on how to apply classification markings, including SCGs, and information on where to access additional classification resources.

The NRC OIG review found that agency derivative classifier training explained principles of derivative classification, classification levels, duration of classification, SCGs, and identification and markings. Derivative classifier training also discussed classification prohibitions and limitations, sanctions, classification challenges, and security.

The Treasury OIG found that some of the classification training materials were outdated and contained incorrect marking instructions. The OIG's review of documents found that 14 of the 30 security education and training documents referenced outdated authorities or provided instructions or information that were

no longer valid. For example, E.O. 12958 was referenced in several training modules even though it was rescinded by E.O. 13526 in 2009. In addition, 18 security training modules had not been updated since 2010. The OIG also found incorrect marking instructions included in recently updated training materials prepared by the central security office.

Conclusions

The 13 OIGs reported having a security education and training program in place. However, the ability to track and manage training certifications varied by agency. Some agencies had not adequately integrated security training requirements into their central training systems. Other agencies had not updated internal guidance to reflect training requirements established by Executive Order 13526 and 32 CFR Part 2001. These issues resulted in knowledge gaps that exist across agencies related to classification markings and challenges to those markings.

Curriculum standards also varied across agencies. In some cases, training did not incorporate all classification requirements. Some agencies successfully fulfilled training requirements while employing a variety of delivery methods. Other agencies still used dated training material or ineffective training methods. Furthermore, some training did not include the necessary information to equip personnel with the requisite knowledge to handle national security information.

Security Self-Inspection Program

This section highlights findings from OIG reports in 2013 and 2016 specific to agency security self-inspection programs. The OIG reports addressed five common themes: representative sampling of documents, records management, frequency of reviews, resource constraints, and agency policy.[20]

[20] Executive Order 13526, section 5.4(d)(4), states that establishing and maintaining an ongoing self-inspection program shall include regular reviews of *representative samples* of the agency's original and derivative classification actions. Records management is the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. Executive Order 13526, section 5.4(c), states that Heads of agencies that originate or handle classified information shall ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and to facilitate its declassification when it no longer meets the standards for continued classification. Executive Order 13526, section 5.4(d)(4), states that establishing and maintaining an ongoing self-inspection program shall include *regular reviews* of representative samples of the agency's original and derivative classification actions. Executive Order 13526, section 5.4(b), states that Heads of agencies that originate or handle classified information shall commit necessary resources for the effective implementation of the CNSI program.

According to Executive Order 13526, section 5.4, each agency component that generated Classified National Security Information (CNSI) is required to establish a self-inspection program. Self-inspections include regular reviews of representative samples of agencies' original and derivative classification actions. According to Executive Order 13526, section 5.4(d)(4), and 32 CFR section 2001.60(c), these samples must encompass all agency activities that generate classified information, and appropriate agency officials must be authorized to correct misclassification actions that are identified. The Senior Agency Official (SAO) is responsible for directing and administering the agency's self-inspection program.

OIGs conducted inspections of agency self-inspection programs and interviewed OCAs, derivative classifiers, and agency security representatives to evaluate their knowledge of classification management procedures. The intent of these inspections and interviews was to determine whether self-inspections were conducted at regular intervals, whether representative samples of original and derivative classified determinations were examined, and whether agency policy was in compliance. Furthermore, OIGs determined whether records of inspections were produced and properly maintained, and if adequate resources were committed to manage the CNSI program and its corresponding requirements.

The problems identified by OIG reviews of the agencies' self-inspection programs are summarized in the following table.

Table 5. Agency OIG Reviews of Self-Inspection Program

Dept./ Agency	Identified Issue(s)		Sampling		Records Mgmt.		Frequency of Reviews		Resource Constraints		Agency Policy	
	2013	2016	2013	2016	2013	2016	2013	2016	2013	2016	2013	2016
DoD	X	X	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	X	X
DHS	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	✓	✓
DOC	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
DOT	X	X	X	X	N/A	X	X	X	X	X	X	X
Energy	X	X	X	X	✓	N/A	X	X	X	X	✓	X
EPA	X	X	N/A	N/A	X	X	N/A	N/A	N/A	N/A	X	N/A
HHS	✓	N/A	✓	N/A	N/A	N/A	✓	N/A	N/A	N/A	✓	N/A
Justice	X	X	X	X	X	X	X	X	X	X	X	✓
NRC	X	X	X	N/A	X	X	X	X	N/A	N/A	X	X
State	X	X	X	X	X	X	X	X	X	X	X	X
Treasury	X	X	X	X	X	X	X	X	X	X	X	X
USAID	X	X	X	X	X	X	X	X	N/A	N/A	X	X
USDA	X	X	X	X	X	X	X	X	X	N/A	X	X

The self-inspection should include reviews of original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight, to ensure compliance with Executive Order 13526 and 32 CFR Part 2001. During self-inspections, components are supposed to examine classified products, e-mail, and presentations for proper classifications and markings.

In 2013, 10 of the 13 OIGs identified discrepancies in their agencies' self-inspection programs. Two OIGs found no discrepancies. Specifically, the OIGs identified issues with sampling of documents, records management, frequency of CNSI program reviews, resource constraints, and policies. One OIG did not address the issue.

The USDA OIG identified problems with how its agency was reporting the self-inspection program to the Information Security Oversight Office (ISOO). The OIG reviewed reports from the previous two fiscal years and found that the

required information was not provided to the ISOO. Specifically, the OIG found that the USDA's FY 2011 and 2012 self-inspection reports did not include:

- a description of the agency's self-inspection program, including activities assessed, program areas covered, and methodology used;
- an assessment and a summary of the findings of the agency's self-inspection program in the following program areas: original classification, derivative classification, declassification, safeguarding, security violations, and management and oversight;
- specific information about the findings of the annual review of the agency's original and derivative classification actions, including the volume of classified materials reviewed and the number and type of discrepancies identified;
- actions that had been taken or were planned to correct identified program deficiencies, marking discrepancies, or misclassification actions, and to deter their reoccurrence; and
- best practices that were identified during self-inspections.

These issues were common with a majority of the OIGs, as discussed below.

The DHS OIG was the only OIG to determine that the self-inspection program was one of the strongest parts of the agency's CNSI program. The OIG verified that the central security office and the 13 components and offices reviewed had conducted self-inspections and sent their findings to senior leadership within the previous 12 months.

In 2016, 10 of the 13 OIGs still identified discrepancies in their agencies' self-inspection programs. One OIG found no discrepancies. Two OIGs did not address the issue.

The USAID OIG's review of the central security office's self-inspection program and 12 agency components (inspected by the central security office and verified through an independent review by the audit team) determined that deficiencies existed in the inspections themselves. Specifically, the OIG made the following determinations:

- Two components did not have any documentation of the inspections, and did not have final inspection reports available.
- One component had documentation of the inspection, but it did not have a final inspection report available.
- No component's inspections included representative sampling, nor did any evaluate declassifications or classified e-mails for compliance with timeliness and marking requirements.

- Five components did not indicate whether they checked to determine whether previous recommendations were implemented.
- One component did not have a designated security officer to ensure that operations were carried out in accordance with policy.
- The central security office's designated security officer, who is responsible for ensuring component compliance with security policies and procedures, was a member of the team conducting the annual self-inspection. This practice creates a conflict of interest and undermines the ability of the central security office to perform inspections with integrity and independence.

In our review of the OIGs' 2016 reports, we found that these issues were common with a majority of the OIGs. Some additional examples are highlighted below.

Sampling

2013

In 2013, eight OIGs identified issues related to self-inspection report sampling procedures. Three OIGs did not identify concerns, and the remaining two did not address this area. At the DoJ, the OIG reviewed a sample of components' self-inspection reports and identified significant errors in methodology. The OIG found that some components reported that they had performed a review of classified documents, but the review procedure described in the report involved only physical security reviews of offices and facilities and did not mention any type of document review.

The DoS reported the results of its first self-inspection of the classification program to the ISOO on January 20, 2012. The OIG reviewed the self-inspection report and found that the agency had generally followed guidance contained in Executive Order 13526, in addition to the guidance provided by the ISOO in its implementing memorandum dated April 5, 2011. However, the sample of derivatively and originally classified documents selected by the agency included Confidential and Secret documents but not Top Secret documents. The OIG concluded that because Top Secret documents were omitted from the self-inspection sample, the results reported to the ISOO were not a true representation of all the agency's classification decisions, and therefore it was impossible to fully evaluate the agency's compliance with principles and requirements of Executive Order 13526 and the effectiveness of

the agency's programs covering original and derivative classifications. Otherwise, the agency followed ISOO guidance in sampling 160 Confidential and Secret agency-prepared documents.

The DoT OIG determined that self-inspection procedures were not adequate and did not fully comply with Executive Order 13526 requirements. The OIG found that in 2010, 2011, and 2012, the agency component did not review any of the 206 derivatively classified documents that were produced, and did not inspect the three primary locations for secure storage of classified information.

The NRC OIG determined that the self-inspections of the agency's CNSI program did not include representative samples of classification decisions in that the component responsible for the CNSI program did not review work produced by classifiers from other components. Although the reviewing component produced nearly half of the classified documents recorded in the agency's tracking database, at least two other components were known to produce classified documents. A fourth component reported producing no hard-copy classified documents even though the office had 13 staff members on the agency's roster of active derivative classifiers. The OIG concluded that expanded self-inspections would improve the agency's oversight of classification activity.

The Treasury OIG reported that for FYs 2011 and 2012, one component generated classified information properly and completed the required self-inspections, while four others either did not complete the self-inspections or completed the inspections but did not retain documentation. The agency's central security office performed and documented self-inspections for those components that generated classified information, but the reviews included only e-mails and attachments. The central security office did not review classified documents generated outside of an electronic environment, and the report sent to the ISOO was based on a review of the central security office's findings. Furthermore, the OIG determined that the agency had established and performed a self-inspection of its CNSI program, as required by Executive Order 13526, but that the self-inspection did not include a representative sample of all classified documents.

The USAID OIG reported that most of the agency's classification actions occur in a classified system, but that central security office employees did not review information in the system. As a result, they did not review most of the agency's original and derivative classification actions.

2016

In 2016, seven OIGs identified issues related to self-inspection report sampling procedures. Two OIGs did not identify concerns, and the remaining four did not address this area. During the compliance followup review, the DoS OIG determined that the central security office had established a process to inspect the agency's classification program, as required by Executive Order 13526. However, the central security office's sample of classified documents for the most recent self-inspection did not include a representative sample of all agency classified documents. Furthermore, the OIG found that the central security office was not capturing all of the collections of classified documents created within the agency as a part of the annual count of classification decisions. The central security office had not fully determined which components had collections of classified documents for the SF 311 data submission to the ISOO.

Records Management

2013

In 2013, seven OIGs identified issues related to the tracking and management of records included in self-inspection reports. Two OIGs did not identify concerns, and the remaining four did not address this area. The DHS OIG determined that records systems were designed and maintained to optimize appropriate sharing and safeguarding of classified information.

The NRC OIG determined that derivative classifiers were not issued training certificates or other documentation after completing required training. OIG staff observed a training session for derivative classifiers and reviewed documents of a previous derivative classifier training session. However, some derivative classifiers interviewed could not accurately recall recent training dates, nor could they produce documentation of their training.

The USDA OIG was unable to verify that components performed self-inspections because central security office staff did not maintain documentation of the self-inspections. The agency reported to the ISOO that 10, 3, and 13 self-inspections had been conducted in FYs 2010, 2011, and 2012, respectively. However, when requested by the OIG, the central security office was able to provide documentation to support only three self-inspections performed in FY 2012. The documentation from component self-inspections was necessary in order for the central security office to track findings and determine whether corrective action had been taken. Without the

self-inspection reports, the OIG was unable to review the findings or corrective actions from the remaining self-inspection reports and concluded that the self-inspection program was ineffective. The staff agreed that improvement was needed in the documentation of the self-inspection program.

2016

In 2016, eight OIGs identified issues related to the tracking and management of records included in self-inspection reports. One OIG did not identify concerns, and the remaining four did not address this area. The NRC OIG determined that document reviews of agency classification actions reported from April 2013 through January 2016 revealed no systematic misclassification. However, the OIG also determined that records management of classified information could be improved. The OIG concluded that the agency lacked a cohesive approach to records management of classified information. For example, the lack of records management of classified information within NRC prevented timely disposition and declassification as required.

The Treasury OIG reported that for FYs 2013 through 2015, three agency components that generated classified information completed the required self-inspections, but one component did not retain the documentation. Furthermore, another component did not complete the self-inspection and informed the central security office that it believed completing the SF 311 met the requirements for self-inspections. The central security did not receive, nor did it request, any self-inspection results.

The USDA OIG determined that its concern from 2013 about maintaining records of self-inspections still had not been addressed, although management indicated that the matter would be resolved by September 30, 2014. Specifically, for FY 2014, the central security office was unable to provide documentation showing any completed self-inspections. For FY 2015, the central security office received self-inspection reports from 8 of 19 components. Agency officials could not explain the reason for the missing self-inspection reports for FYs 2014 or 2015. A June 9, 2016, policy memorandum included a requirement that all components conduct self-inspections annually, no later than the second week of August, and submit self-inspection reports to the central security office within 30 days of completion. It further directed that the self-inspection reports be maintained for 2 years.

Frequency of Reviews

2013

In 2013, eight OIGs identified issues related to the frequency of required self-assessments and classification decision reviews. Two OIGs did not identify concerns, and the remaining three did not address this area. The DoE OIG determined that responsible officials had not conducted the required biennial self-assessments and annual classification decision reviews. Classification officials reviewed only 140 finished intelligence products during FY 2012. Classification officials did not review e-mails and internal documents, despite the fact that 90 percent of the 5,737 derivative classifier decisions reported to the ISOO related to e-mails. In addition, annual classification decision reviews excluded field intelligence element activities. A classification decision review was conducted at one of two field intelligence sites reviewed in conjunction with an onsite evaluation in 2012. The review was last performed in 2012, even though it is required on an annual basis. The OIG determined that the lack of annual classification decision reviews may have contributed to classification marking errors identified during the review.

The DoJ OIG verified that some security program managers conducted informal reviews but these reviews did not include an evaluation of the classification and marking of documents. In addition, some components did not conduct annual reviews, as directed, but conducted reviews on a triennial basis. Moreover, some components did not answer all of the questions included in the self-inspection checklist, which could result in an incomplete self-inspection review.

The DoT OIG reported that agency officials stated that in 2013 they began a more comprehensive self-inspection program that included inspecting some of their major components. Officials indicated that once the initial review was completed, they would share the results with the OIG. The OIG determined that without comprehensive self-inspections the agency cannot know whether documents are properly classified and protected.

2016

In 2016, eight OIGs identified issues related to the frequency of required self-assessments and classification decision reviews. One OIG did not identify concerns, and the remaining four did not address this area. The DoE OIG determined that the agency's central security office had made some progress in completing the

oversight reviews required by policy, but it had conducted only 37 percent of its required annual classification decision reviews and 73 percent of its required biennial classification program self-assessments.

The Treasury OIG determined that a central security office representative did not know why the office did not have copies of component self-inspection results. For FY 2015, the representative stated that the central security office did not follow up on the self-inspection results because the staff was busy with another security oversight and assessment program.

Resource Constraint

2013

In 2013, six OIGs identified resource constraints as an impediment to effective self-inspections. Seven OIGs did not address this area. The DoT OIG reported that agency officials asserted that they did not have sufficient resources to effectively conduct self-inspections, and that only one person was assigned to conduct self-inspections.

The USDA OIG determined that although staff tried to gather missing self-inspection information, because of resource constraints the agency allowed components to complete the self-inspection and send in their results. The agency acknowledged that in some cases, it might not have received all the self-inspection results.

2016

In 2016, five OIGs identified resource constraints as an impediment to effective self-inspections. Eight OIGs did not address this area. The DoJ OIG reported that the agency's central security office had been unable to consistently implement its enhanced process for reviewing component self-inspection reports. The central security office reported that, because of resource constraints, it continued to experience difficulties in executing internal control procedures over self-inspections and classification reporting requirements. As a result, the central security office was not consistently ensuring that all reportable classification information was complete and accurate.

The DoT OIG determined that one agency component's self-inspection procedures did not fully comply with Executive Order 13526 requirements, primarily because the central security office was not dedicating sufficient resources to overseeing the component's self-inspection program. At the five locations in the OIG sample,

the OIG did not find evidence to support reviews of original or derivative classification actions. The OIG also noted some cases in which the inspection revealed errors (for example, overdue changes to safe combinations); yet, the inspection report stated, "There were no findings noted during this inspection." Agency management was unaware of these errors before the OIG review. Without comprehensive or accurate self-inspections, the component cannot ensure that documents are properly classified, handled, and protected.

Policy

2013

In 2013, nine OIGs identified issues related to self-inspection program policy. Three OIGs did not identify concerns, and the remaining OIG did not address this area. The NRC OIG determined that even though agency policy called for a self-inspection program, the policy did not reflect current Federal standards. Specifically, the agency's guidance did not call for representative sampling of classifications and correction of misclassifications. Although the central security office was responsible for the agency's CNSI program, the wording of agency policy did not provide the central security office the necessary authority to conduct broader scoped self-inspections.

The USDA OIG reported that agency policy did not address coverage and external reporting when conducting self-inspections.

2016

In 2016, five OIGs identified resource constraints as an impediment to effective self-inspections. Eight OIGs did not address this area. The Treasury OIG determined that the agency updated security policy in 2013 and required components to report self-inspection results to the central security office. However, the policy did not include procedures for the central security office to follow up on the self-inspection reports.

Conclusions

The OIGs' reports found that self-inspection reports were not consistently comprehensive or conducted when required. At some agencies, the classified documents that were reviewed during self-inspections did not amount to a representative sample of all agency-classified documents. In addition, some agencies had not captured all of the collections of classified documents created within the

agency as part of the annual count of classification decisions and had not fully determined which components had collections of classified documents for the SF 311 data submission to the ISOO.

Resource constraints were often cited as a reason for incomplete reporting of information to the ISOO. In some instances, OIGs were unable to verify that components performed self-inspections because agency security staff did not maintain documentation of the self-inspections.

Without routine self-inspections, violations of security requirements may go undetected. Such vulnerabilities could lead to inappropriate release or inappropriate restriction of classified information.

Security Reporting

Executive Order 13526, section 5.4(d)(4), and 32 CFR section 2001.90 require that each agency that creates or safeguards classified information annually report security classification program statistics to the ISOO.

This section focuses on the manner in which statistics on the state of agency CNSI programs were compiled and the reliability of information reported to the ISOO. OIGs examined program effectiveness by evaluating the accuracy of statistical reporting on the SF 311, the Fundamental Classification Guidance Review (FCGR), and self-inspection results, as reported to the ISOO.[21] The ISOO analyzes the information and submits an annual report to the President, that includes the cost of security classification activity. The problems identified by the OIG reviews of the agencies' security reporting programs are summarized in the following table.

[21] SF 311s report the total number of OCAs, classification decisions, mandatory review requests, and declassification decisions for an agency. Self-inspections evaluate the effectiveness of agency CNSI programs. The FCGR entails a comprehensive review of agency classification guidance. Additional information on SF 311s, self-inspections, and the FCGR can be found in the "Summary of Findings" and "Background" sections of this report.

Table 6. Agency OIG Reviews of Security Reporting

Dept./ Agency	Identified Issue(s)		Intra-agency Methodologies		Component Calculations		Agency Verification		Guidance	
	2013	2016	2013	2016	2013	2016	2013	2016	2013	2016
DoD	X	N/A	X	N/A	X	N/A	✓	N/A	X	N/A
DHS	X	✓	X	✓	N/A	N/A	N/A	N/A	X	N/A
DOC	X	X	N/A	N/A	N/A	N/A	X	X	X	X
DOT	X	X	X	✓	X	✓	X	✓	X	X
Energy	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
EPA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
HHS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Justice	X	X	X	X	X	X	X	X	X	X
NRC	X	✓	X	✓	N/A	N/A	N/A	N/A	X	✓
State	X	X	X	X	N/A	N/A	X	X	X	N/A
Treasury	X	X	X	X	X	X	X	X	X	X
USAID	X	X	X	X	X	N/A	N/A	X	N/A	N/A
USDA	X	X	N/A	N/A	X	N/A	X	X	X	X

Statistical Reporting

In 2013, 10 of the 13 OIGs identified discrepancies in SF 311 reports with respect to the manner in which statistics were compiled and the reliability of information reported. Three OIGs did not address the issue.

Agencies employed disparate methods for collecting and estimating data, using different assumptions about what should be included. In addition, several OIGs found inconsistent applications of ISOO requirements and inconsistent definitions of what annual reports should include. The 11 OIGs that reported discrepancies identified four general areas of concern related to security reporting—differing methodologies, incorrect calculations, lack of verification, and inadequate understanding of guidance.[22]

[22] Methodologies refers to the manner in which data were collected, internal to an agency at the component level. Incorrect calculations reflects how, once collected, the data were counted. Verification issues occurred at the agency level where information was not consistently evaluated for accuracy. Identified guidance issues included the absence of detailed instructions on how to compile and calculate data for inclusion in annual reports to the ISOO.

Although some agencies implemented corrective measures in 2016, 7 of the 13 OIGs still identified issues in four general areas of concern—methodology, verification, guidance, and calculations. Four OIGs did not address the issue in 2016. Two OIGs determined that recommendations were satisfactorily implemented. Specific examples from both reporting periods are discussed below.

Intra-agency methodologies

2013

In 2013, eight OIGs identified issues related to the manner in which data were collected for security reports. Five OIGs did not address this area. According to the DHS OIG report, the agency provided all statistical reports to the ISOO on classification activities, costs, FCGR reviews, self-inspections, and security violations in a timely manner. However, security managers believed that the estimates on the SF 311s were not entirely accurate due to overly broad directions. The OIG found that although the central security office provided general directions on using the forms, each component and office had its own system for compiling statistics. Without a standard way to collect statistics, the agency may not have reported a true representation of its classified holdings or decisions.

The DoD OIG found that the agency's annual estimates of original and derivative classification decisions were unreliable because those estimates were based on component data that were derived using different assumptions about data collection and estimating techniques, including what should be included.

2016

In 2016, four OIGs identified issues related to the manner in which data were collected for security reports. Three OIGs did not identify concerns. Six OIGs did not address this area. The DHS OIG found that the agency modified its method for collecting and reporting classification management data on the SF 311 to ensure internal consistency. The central security office proposed standard procedures to count the agency's classification decisions. The new procedures decreased the reporting period from 12 months to 3 months (April to June) to encourage users to focus on tracking classification decisions during this period. To standardize and simplify the collection process, the agency used the SF 311A, which provides specific accounting instructions for recording individual classification decisions. The OIG determined that the agency continued to follow these standard procedures to track classification decisions.

The DoJ OIG reviewed self-inspection reports and determined that one component's FY 2015 submissions included inaccurate information related to classification training. According to the security manager who performed the component's self-inspection, the agency's report contained more complete and accurate information than previous reports. In an earlier report, the component reported that it provided initial security training to 100 percent of its employees with security clearances. In a later report, the component reported that it provided this training to 42 percent of employees with security clearances. The OIG reported that although the security manager stated that he could not speak directly to the accuracy of the earlier submission, he stated that the component had never developed or implemented initial security training for new employees who are non-core personnel. The OIG concluded that it would not have been possible for the component to have a 100 percent completion rate as reported in the earlier submission.

Calculations

2013

In 2013, 6 OIGs identified concerns with the manner in which components estimated original and derivative classification decisions. Seven OIGs did not address the issue. The Treasury OIG determined that the Treasury did not provide the ISOO with a complete and accurate count of its overall derivative and original classification decisions on the SF 311 for fiscal years 2011 and 2012. For 2011, 12,733 derivative classification decisions were reported to the ISOO. However, when a mathematical check of the internally submitted data was performed by the OIG the total was much smaller—only 6,123 decisions. For 2012, 20,179 derivative classification decisions were reported to the ISOO, but once the internally submitted reports were recalculated by the OIG, the total was 20,076 decisions. Agency totals reported to the ISOO for these reporting years also did not include derivative classification decision counts for one particular office that regularly handles classified information.

The USDA OIG found that the comprehensive SF 311s the agency submitted to the ISOO contained unsupported data that conflicted with the data submitted in component SF 311s. In addition, the central security office did not document in the SF 311 how it calculated estimated statistics for derivative classification decisions. Additionally, when requested by the OIG, staff members were unable to determine how the calculations were performed and could not provide documentation to support the estimate.

2016

In 2016, two OIGs identified concerns with the manner in which components estimated original and derivative classification decisions. One OIG did not report any discrepancies. The remaining 10 OIGs did not address the issue in their 2016 reports. The Treasury OIG performed a check of the number of classification decisions reported on the SF 311s that the agency's components submitted to the central security office for three consecutive years, following the first audit, and compared them to the consolidated SF 311s prepared by the central security office. The analysis identified discrepancies in the numbers of derivative and original classification decisions reported to the ISOO. A central security office representative could not explain the differences between the sum of component SF 311s and the total on the consolidated SF 311 reported to the ISOO. The central security office had reported original classification decisions for the three consecutive years as zero, 10, and 30, respectively. However, when the OIG verified the count with internally submitted data from the components to the central security office, a single component had reported 14 decisions for the first year.

Verification

2013

In 2013, six OIGs identified discrepancies in the manner in which security data were verified. One OIG did not identify concerns, and six OIGs did not address the issue. As an example, the DoJ OIG found that the agency annually prepared and submitted to the ISOO certain metrics on classification training, the number of classification decisions, the number of challenges to agency classification decisions, and the associated costs of maintaining classified agency information. The agency relied on the components to self-report the above information. However, the OIG found that the agency had not verified the accuracy of the information reported, even though some of the information submitted by components was questionable on its face.

2016

In 2016, six OIGs identified discrepancies in the manner in which security data were verified. One OIG did not identify concerns, and six OIGs did not address the issue.[23] As an example, the DoJ OIG found that after the 2013 report, the agency revised the

[23] The 2013 and 2016 totals remain the same for three reasons. USAID did not address the matter in 2013 but identified concerns in its 2016 report. DoD had positive findings in its 2013 report and did not address this area in its 2016 report. DoT found discrepancies in 2013 but noted improvements in its 2016 report.

processes for evaluating components' self-inspection reports to improve the accuracy of the information reported to the ISOO. However, the OIG found that the central security office did not implement the enhanced process consistently. As a result, self-inspection reporting contained deficiencies and inaccuracies. Central security office officials stated that resource constraints continued to hinder their ability to manage the agency's classification program effectively and efficiently.

The USDA OIG determined that for two consecutive years of reporting following the 2013 audit, the agency documented 680 and 1,464 derivative classification decisions for FYs 2014 and 2015 respectively. However, the SF 311s provided by the agency components supported 634 decisions for FY 2014. For FY 2015, the agency reported derivative classification decisions, but the SF 311s the components provided supported only 744 decisions. The central security office was not able to explain or provide support for the differences. The agency had agreed to take actions in response to findings in the 2013 audit report. However, the OIG concluded that the agency had not developed and implemented internal controls to minimize the risk of over-classifying or improperly releasing CNSI. The OIG stressed the need for senior leadership to monitor and oversee activities and ensure that adequate internal controls were developed and implemented.

Guidance

2013

In 2013, nine OIGs determined that agency guidance was not sufficient to support the accurate reporting of classified decisions. Four OIGs did not address this area. At DoJ, the OIG found that components did not receive adequate guidance on how to report the number of classified decisions. Some component officials acknowledged that they reported an incorrect number of classified decisions because they were unclear about the reporting requirements.

The DoS OIG found that the process used to determine the number of derivative decisions made confirmed that the numbers reported were inaccurate because the component had not followed the guidance provided by the ISOO on how to count or estimate classified e-mails.

2016

In 2016, five OIGs determined that agency guidance was not sufficient to support the accurate reporting of classified decisions. One OIG did not identify any concerns. Seven OIGs did not address this area. The USDA OIG concluded in its 2013 audit that the agency had not effectively gathered information and reported statistics related to its security classification program. The OIG recommended that the central security office develop instructions to provide to agency components with instructions on how to document statistical information used to substantiate information in the annual report to the ISOO. The OIG found that the agency had not issued final guidance requiring reports to be submitted on an annual basis. Furthermore, the central security office provided components with the instructions from the ISOO, instead of developing guidance specific to the agency to assist the components in completing the statistical report. Because the agency implemented inadequate corrective actions, the OIG found that there were still discrepancies between the number of derivative decisions reported to the central security office by the components, and the number that the central security office reported to the ISOO.

Conclusions

While OIGs made recommendations in their 2013 reports to address concerns with methodology, verification, guidance, and calculations, corrective measures taken by the agencies did not consistently address these issues. The OIGs identified discrepancies in SF 311 reports with respect to the manner in which statistics were compiled and the reliability of information reported in both 2013 and 2016.

The OIGs also found inconsistent applications of the ISOO's requirements and inconsistent definitions of what annual reports should include. OIGs also noted that components within agencies employed disparate methods for collecting and estimating data, using different assumptions about what should be included.

Inconsistencies identified by the OIGs included disparate sampling methodologies, variances in totals reported for derivative classification decisions, failure of subordinate components to provide relevant information or documentation, and incomplete data reviewed for inclusion in reports.

Agency SF 311s submitted to the ISOO also contained unsupported data that, at times, conflicted with the data submitted to central security offices by agency components. As a result, the ISOO may have received and relied upon incomplete or inaccurate information concerning the status of agency CNSI programs. Without a standard way to collect statistics, agencies may not be able to report a true representation of their classified holdings or decisions, and they may not be able to allocate sufficient resources to adequately protect CNSI.

General Administration

According to Executive Order 13526, the administration of CNSI requires effective policies and consistent organizational oversight. Agencies are required to incorporate accountability for the creation and handling of classified information into performance plans and evaluations. Agencies should have guidance, processes, and training for derivative classifiers to facilitate classification challenges. In addition, according to the Executive order incentives and sanctions should be in place to ensure the proper handling of classified information.

Some OIGs identified issues related to performance evaluations and classification challenges. However, none of the OIGs identified an occurrence when its agency provided incentives to employees for accurate classification. Moreover, none of the OIGs identified an occurrence when an agency imposed sanctions for inappropriate classification decisions or noncompliance. The problems identified by the OIG reviews of the agencies' general administration programs are summarized in the following table.

Table 7. Agency OIG Reviews of General Administration

Dept./ Agency	Identified Issue(s)		Performance Evaluations		Classification Challenges		Incentives Given and Sanctions Imposed	
	2013	2016	2013	2016	2013	2016	2013	2016
DoD	X	X	X	X	X	X	N/A	N/A
DHS	✓	N/A	N/A	N/A	✓	N/A	N/A	N/A
DOC	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
DOT	N/A	X	N/A	X	N/A	N/A	N/A	N/A
Energy	X	✓	X	N/A	X	✓	N/A	N/A
EPA	X	✓	X	✓	N/A	N/A	N/A	N/A
HHS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Justice	X	X	X	X	X	N/A	N/A	N/A
NRC	X	N/A	X	N/A	N/A	N/A	N/A	N/A
State	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Treasury	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
USAID	N/A	X	N/A	N/A	N/A	X	N/A	N/A
USDA	X	N/A	N/A	N/A	X	N/A	N/A	N/A

Performance Plans and Evaluations

Executive Order 13526 requires that performance plans and evaluations for personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings, contain the designation and management of classified information as a critical performance element.[24]

[24] Executive Order 13526, section 5.4(d)(7), requires heads of agencies that originate or handle classified information to ensure that the performance contract or other system used to rate civilian or military personnel performance include the designation and management of classified information as a critical element or item to be evaluated in the rating of: (A) original classification authorities; (B) security managers or security specialists; and (C) all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings.

2013

In 2013, 5 of the 13 OIGs identified problems with personnel not having a critical element on security in their performance evaluations. The five OIGs determined that some agency components had a critical element on security in the performance evaluations for their personnel, while other components did not.

For example, the DoD OIG determined that some agency components had a critical element on security in their staff performance plans, while others did not.

The DoE OIG determined that performance standards regarding classification duties had not been established for the majority of derivative classifiers interviewed.

The DoJ OIG determined that not all agency components incorporated classification management into performance plans and evaluations for OCA officials, derivative classifiers, and security programs officials.

The EPA OIG determined that not all cleared personnel who required it had an element or item relating to designation and management of classified information in their performance evaluation. Specifically, EO 13526 requires such an element or item to be evaluated in the rating for personnel whose duties significantly involve handling classified information, including those who regularly apply derivative classification markings. In some instances, when performance plans and appraisal records were reviewed, those employees whose duties involved significant handling of classified information did have a critical element on classified material handling that met the requirements of Executive Order 13526.

The NRC OIG determined that most derivative classifiers did not have classification duties in their position descriptions and were not rated on these tasks. Among the nine derivative classifiers interviewed, six stated that they did not have classification duties in their position descriptions, and seven indicated that they were not evaluated on classification duties. Some noted that they had been evaluated on classification duties in the past, and some cautioned that it is difficult to weigh classification duties proportionally to other core job tasks and responsibilities.

2016

In 2016, 3 of the 13 OIGs still identified discrepancies, 1 OIG determined that improvements were made, and 9 of the 13 OIGs did not address the issue.

For example, the DoD OIG found that based on a survey it conducted, 1,630 of the 1,988 (82 percent) original and derivative classifiers surveyed had a critical element on security in their performance evaluations. However, 18 percent still did not.

The DoJ OIG, based on its review of the agency's self-inspection reports, determined that although a central security office memorandum to all agency components required incorporating classification management into performance plans and evaluations, not all components had done so.

The DoT OIG determined that one of two agency components complied with the requirement to include a critical element on security in the performance evaluation of all employees whose duties significantly involve the creation, handling, or management of classified information. The OIG obtained performance plan templates or performance plans for all sites in the sample of the second component and found that none of the performance plans contained the critical element.

The EPA OIG determined that the agency's central security office provided standard wording for a critical job element to be part of the performance evaluation of employees with a security clearance.

Conclusion

Although compliance with the requirement to have a critical element on security in the performance evaluations of derivative classifiers improved from 2013 to 2016, additional improvements are needed. Without the critical element for security in performance evaluations, there is little accountability for ensuring the proper marking and classification of documents.

Challenges to Classification

According to Executive Order 13526, section 1.8, and 32 CFR section 2001.14, derivative classifiers who want to challenge the level at which information is classified are encouraged and expected to challenge that status. Agencies are required to establish formal processes to allow such challenges.[25] According to Executive Order 13526, section 5.3, the individual submitting the challenge has a right to appeal the decision to the Interagency Security Classification Appeals Panel or the Chief Security Officer acting as the SAO, who convenes a Classification Appeals Panel.[26]

2013

In 2013, 5 of the 13 OIGs addressed challenges to inappropriately classified documents in their reports. One OIG reported positive findings. Four OIGs identified issues of concern. Eight OIGs did not address the issue. OIGs determined that policy and training on the process for formally or informally challenging improperly classified documents needed to be strengthened. However, the DHS OIG determined that all interviewees knew the process of formal or informal challenges.

The DoD OIG determined that policy did not require language in SCGs encouraging challenges and providing citations to assist in the challenge process (only 37.5 percent of SCGs included guidance for individuals who want to challenge or question the level of classification). Nonetheless, some interviewees who made classification challenges stated that they were satisfied with how the challenge was resolved. Interviewees also stated that their training successfully addressed classification challenges.

The DoE OIG determined that some derivative classifiers were not familiar with the requirements for making a formal challenge to external entities when they believe that information may be misclassified. However, interviewees stated that they were aware of their responsibility to reach out internally to their respective classification officers. The OIG also interviewed derivative classifiers and determined that they were

[25] Formal challenges must be written and presented to an OCA with jurisdiction over the challenged information. The OCA then must provide a written classification or declassification decision to the challenger within 60 days of receipt. Individuals who challenge classifications are not to be subject to retribution. Challengers' requests for anonymity are honored, and they have a representative to serve as their agent in processing the challenge. There is also a secure capability to receive information, allegations, or classification challenges.

[26] The Interagency Security Classification Appeals Panel consists of the Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Adviser. Senior-level representatives, who are full-time or permanent part-time Federal officers or employees, serve as members of the Panel, designated by the respective agency head. The President shall designate a Chair from among the members of the Panel. The Director of the ISOO serves as the Executive Secretary of the Panel. The staff of the ISOO provides program and administrative support for the Panel.

not familiar with all requirements for making a formal challenge regarding information that may be misclassified because the agency had not developed training and guidance on the requirements for making a formal challenge.

The DoJ OIG determined that many agency officials were unaware of the agency's process for challenging classifications, and that some policies did not explicitly include a statement that all individuals are protected from retribution for challenging the classification of information.

The USDA OIG determined that the agency's policy did not adequately advise individuals of their rights to appeal to the Interagency Security Classification Appeals Panel. The OIG also found that the policy did not include the timeframes for challenges to be forwarded to the appeals panel. Some officials disagreed that the policy did not adequately advise individuals of their right to appeal. They cited agency policy that required classification challenges to be resolved to the extent possible within 30 calendar days of receipt of a challenge. However, the OIG recommended that the policy be updated so that classifiers are aware of the appeals process and timeframe for sending matters to the appeals panel.

2016

Only three OIGs addressed challenges to classification in 2016. One OIG identified improvement. The remaining two OIGs identified improved processes, but determined that some aspects of policies at these two agencies still needed to be updated.

For example, during a followup review, the DoD OIG reported improvement in the agency's challenge process and found that 103 of 109 SCGs reviewed included some guidance on challenges. This represents a 94-percent compliance rate with existing agency policy and is consistent with guidance provided in Executive Order 13526, that authorized holders of classified information should be able to challenge the classification status of the information in accordance with agency procedures. Additionally, 1,988 derivative classifiers were asked whether they were aware that agency policy encouraged challenges if the classifiers believe the information is incorrectly classified. The OIG found that 83 percent of those surveyed (1,644) were aware that agency guidance encouraged challenges, while 17 percent were

not aware. Moreover, 135 survey participants indicated that they challenged classification levels through formal processes (contacting the office of primary responsibility) or informal channels (seeking clarification). Of the SCGs reviewed, the OIG still found instances in which challenge language was not consistent with guidance provided in Executive Order 13526 and 32 CFR section 2001.14.

The USAID OIG reported that procedures for challenging classification did not state that employees are protected from retribution and did not provide deadlines that the agency must meet for responding to challenges, including appeals.

Incentives and Sanctions

Public Law 111-258, section 6(a), allows agencies to provide incentives to classifiers to make appropriate classification decisions and to challenge classification decisions that the employees believe are inappropriate. Conversely, Executive Order 13526, section 5.5, outlines sanctions for inappropriate classification decisions and classifiers who knowingly, willfully, or negligently fail to comply with classification and safeguarding requirements.[27] However, none of the OIGs identified an occurrence when its agency provided incentives to employees for accurate classification. Moreover, none of the OIGs identified an occurrence when an agency imposed sanctions for inappropriate classification decisions or noncompliance.

Incentives

Public Law 111-258, section 6(a), states that cash awards are available as incentives for accurate classification of CNSI. No OIG reported that its agency provided cash awards to any employee for accurate classification.

The USDA OIG reported that the agency did not offer incentives to encourage accurate classification or declassification because classification of information by the OCA is an in-depth process and proper classification management was addressed through user training and awareness.

[27] Sanctions may include reprimand, suspension without pay, removal, termination of classified authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

Sanctions

Executive Order 13526, sections 4.1 and 5.5, state that criminal, civil, and administrative sanctions may be imposed on an individual who fails to protect CNSI from unauthorized disclosure. Every person who has met the standards for access to classified information must receive training on the proper safeguarding of CNSI and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

No OIG reported on the imposition of agency sanctions for inappropriate classification decisions or noncompliance.

Conclusion

Agencies and their derivative classifiers reported that they were knowledgeable about possible sanctions for mishandling classified information. Organizational policy and training addressed sanctions, but no agency reported that it had imposed sanctions.

APPENDIX A

Scope and Methodology

Scope

Public Law 111-258 requires OIGs of Federal departments, or agencies with an officer or employee who is authorized to make original classifications, to: (A) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and (B) identify policies, procedures, rules, regulations or management practices that may be contributing to persistent misclassification of material. This includes an assessment of the policies and guidance issued by each agency as part of the scope. Public Law 111-258 was designed not only to reduce or prevent over-classification of information, but to minimize the over-compartmentalization of information, while promoting the sharing and declassifying of information as prescribed by Federal guidelines.

Methodology

An evaluation guide was prepared for use by all OIGs participating in this Government-wide assessment effort. The guide, to meet the requirements of Public Law 111-258, was created by a working group from the OIGs that was formed to ensure consistency in the evaluative process and comparable reporting. The evaluation guide, "A Standard User's Guide for Inspectors General Conducting Evaluations under Public Law 111-258, the Reducing Over-Classification Act," can be found on the CIGIE website: www.ignet.gov/CIGIE Reports and Periodicals/List by Year/2013/.

As directed by the Act, the DoD OIG consulted with the ISOO and coordinated with other OIGs to ensure that the OIGs' assessments followed a consistent methodology to allow for cross-agency comparisons. To accomplish this consistent methodology, agency OIGs:

- examined the results of the Fundamental Classification Guidance Review (FCGR);
- examined the results of self-inspection reporting;
- examined SF 311s, "Agency Security Classification Management Program Data";
- reviewed relevant policies, regulations, and related studies;
- reviewed 3,797 classified documents;

- interviewed and surveyed 2,742 component security managers and original and derivative classifiers; and
- interviewed key agency officials responsible for security training and related policy development and implementation.

The OIGs' assessments focused on original classification authority; general program management responsibilities; original classification; derivative classification; self-inspections; security reporting; security education and training; performance evaluations; challenges to classification; and incentives and sanctions.

To assess whether agency policies and practices were consistent with Executive Order 13526 and 32 CFR Part 2001, the OIGs used assessment tools developed by the ISOO. Specifically, the OIGs used:

- an agency regulation implementing assessment tool,
- a methodology for determining the appropriateness of an original classification decision,
- a methodology for determining the appropriateness of a derivative classification decision,
- derivative classifier interview questions, and
- original classification authority interview questions.

APPENDIX B

Prior Coverage

Department of Agriculture

- Report No. 61701-0001-32, "U.S. Department of Agriculture's Office of Homeland Security and Emergency Management Coordination—Classification Management," September 2013
- Report No. 61701-0001-23, "Fiscal Year 2016 Classification Management," September 2016

Department of Commerce

- Report No. OIG-13-031-A, "Classified Information Policies and Practices at the Department of Commerce Need Improvement," September 30, 2013
- Report No. OIG-16-048-A, "Follow-up Audit on Recommendations From Audit Report No. OIG-13-031-A, "Classified Information Policies and Practices at the Department of Commerce Need Improvement," September 30, 2016

Department of Defense

- Report No. DODIG-2013-142, "DoD Evaluation of Over-Classification of National Security Information," September 30, 2013
- Report No. DODIG-2017-028, "Follow up to DoD Evaluation of Over-Classification of National Security Information," December 1, 2016

Department of Energy

- Report No. DOE/IG-0904, "Review of Controls Over the Department's Classification of National Security Information," March 2014
- Report No. DOE-OIG-17-04, "Followup Review of Controls Over the Department's Classification of National Security Information," January 2017

Department of Health and Human Services

- Report No. OEI-07-12-00400, "HHS Adopted, Administered, and Generally Followed Classified Information Policies," May 2013
- Report No. OEI-07-12-00401, "Originally and Derivatively Classified Documents Met Most Federal Requirements," May 2013
- Report No. OEI-07-16-00080, "HHS Has Made Progress in Properly Classifying Documents; However, New Issues Should be Addressed," September 2016

Department of Homeland Security

- Report No. OIG-13-106, "Reducing Over-classification of DHS' National Security Information," August 2013
- Report No. OIG-16-141, "DHS Has Not Trained Classified Network Users on the Classification Management Tool," September 26, 2016

Department of Justice

- Report No. 13-40, "Audit of the Department of Justice's Implementation of and Compliance with Certain Classification Requirements," September 2013
- Report No. 16-26, "Follow-up Audit of the Department of Justice's Implementation of and Compliance with Certain Classification Requirements," September 2016

Department of State

- Report No. AUD-SI-13-22, "Evaluation of Department of State Implementation of Executive Order 13526, Classified National Security Information," March 2013
- Report No. AUD-SI-16-43, "Compliance Follow up Review of the Department of State's Implementation of Executive Order 13526, Classified National Security Information," September 2016

Department of Transportation

- Report No. FI-2013-136, "DOT Does Not Fully Comply with Requirements of the Reducing Over-Classification Act," September 19, 2013
- Report No. FI-2017-006, "Improvements Increase DOT's Compliance with Requirements of the Reducing Over-Classification Act," November 7, 2016

Department of the Treasury

- Report No. OIG-13-055, "Treasury Has Policies and Procedures to Safeguard Classified Information But Implementation Needs to Be Improved," September 27, 2013
- Report No. OIG-16-059, "Treasury Has Policies and Procedures to Safeguard Classified Information But They Are Not Effectively Implemented," September 29, 2016

Environmental Protection Agency

- Report No. 11-P-0722, "EPA Should Prepare and Distribute Security Classification Guides," September 29, 2011
- Report No. 12-P-0543, "EPA's National Security Information Program Could Be Improved," June 18, 2012
- Report No. 14-P-0017, "EPA Does Not Adequately Follow National Security Information Classification Standards," November 15, 2013
- Report No. 16-P-0196, "EPA Improved Its National Security Information Program, but Some Improvements Still Needed," June 2, 2016

Nuclear Regulatory Commission

- Report No. OIG 13-A-21, "Audit of NRC's Implementation of Federal Classified Information Laws and Policies," September 12, 2013
- Report No. OIG 16-A-17, "Audit of NRC's Implementation of Federal Classified Information Laws and Policies," June 8, 2016

U.S. Agency for International Development

- Report No. 9-000-14-002-S, "Evaluation of USAID's Implementation of Executive Order 13526, Classified National Security Information," July 25, 2014
- Report No. 9-000-16-001-P, "USAID's Implementation of Executive Order 13526, Classified National Security Information, Needs Significant Improvement," September 30, 2016

APPENDIX C

Intelligence Community Reporting

The Inspector General of the Intelligence Community also conducted a review and analysis of the 2013 reports from the OIGs of each Intelligence Community agency to identify systemic issues related to classification in the Intelligence Community.[28] The results of this review are contained in Report Number INS-2014-002, "Evaluation of the Office of the Director of National Intelligence Under the Reducing Over-Classification Act," December 30, 2014.

The Intelligence Community IG identified three key areas requiring emphasis across the Intelligence Community—training, program management, and oversight. The three areas are summarized as follows:

- Training:
  - Two OIG reports noted that less than half of the workforce met the recurring biennial training requirement, while two others noted that their agencies did not measure compliance with this requirement.
  - Five of the six OIG reports found their agency's training for derivative classifiers did not adequately prepare those personnel to make derivative classification decisions.
- Program Management:
  - All six OIG reports noted that their agency's self-inspection program did not fully comply with the Executive Order 13526 requirements.
- Oversight:
  - One OIG report noted that its agency did not assess appropriate performance metrics as part of its oversight of the Intelligence Community classification markings program.

[28] The Intelligence Community OIGs included in the report were from the following agencies: Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Security Agency, National Reconnaissance Office, and Office of the Director of National Intelligence.

APPENDIX D

Section 6(b), Public Law 111-258–Inspector General Evaluations

SEC. 6. PROMOTION OF ACCURATE CLASSIFICATION OF INFORMATION.

(b) INSPECTOR GENERAL EVALUATIONS.—

(1) REQUIREMENT FOR EVALUATIONS.—Not later than September 30, 2016, the inspector general of each department or agency of the United States with an officer or employee who is authorized to make original classifications, in consultation with the Information Security Oversight Office, shall carry out no less than two evaluations of that department or agency or a component of the department or agency—

(A) to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and

(B) to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency or component.

(2) DEADLINES FOR EVALUATIONS.—

(A) INITIAL EVALUATIONS.—Each first evaluation required by paragraph (1) shall be completed no later than September 30, 2013.

(B) SECOND EVALUATIONS.—Each second evaluation required by paragraph (1) shall review progress made pursuant to the results of the first evaluation and shall be completed no later than September 30, 2016.

(3) REPORTS.—

(A) REQUIREMENT.—Each inspector general who is required to carry out an evaluation under paragraph (1) shall submit to the appropriate entities a report on each such evaluation.

(B) CONTENT.—Each report submitted under subparagraph (A) shall include a description of—

(i) the policies, procedures, rules, regulations, or management practices, if any, identified by the inspector general under paragraph (1)(B); and

(ii) the recommendations, if any, of the inspector general to address any such identified policies, procedures, rules, regulations, or management practices.

(C) COORDINATION.—The inspectors general who are required to carry out evaluations under paragraph (1) shall coordinate with each other and with the Information Security Oversight Office to ensure that evaluations follow a consistent methodology, as appropriate, that allows for cross-agency comparisons.

(4) APPROPRIATE ENTITIES DEFINED.—In this subsection, the term ''appropriate entities'' means—

(A) the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate;

(B) the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Permanent Select Committee on Intelligence of the House of Representatives;

(C) any other committee of Congress with jurisdiction over a department or agency referred to in paragraph (1);

(D) the head of a department or agency referred to in paragraph (1); and

(E) the Director of the Information Security Oversight Office.

ACRONYMS AND ABBREVIATIONS

CFR Code of Federal Regulations
CIGIE Council of the Inspectors General on Integrity and Efficiency
CMT Classification Management Tool
CNSI Classified National Security Information
FCGR Fundamental Classification Guidance Review
ISOO Information Security Oversight Office
OCA Original Classification Authority
SAO Senior Agency Official
SCG Security Classification Guide

Council of the
INSPECTORS GENERAL
on INTEGRITY *and* EFFICIENCY

Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

MISSION, VISION, AND VALUES

Improving government–wide efficiency, effectiveness, and integrity and enhancing the professionalism of CIGIE members.

VISION

Advancing good government through collaboration.

VALUES

- Integrity
- Accountability
- Transparency
- Collaboration
- Excellence

Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

www.ignet.gov