Department of Homeland Security

Office of Inspector General

Reducing Over-classification of DHS' National Security Information

OIG-13-106

August 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

August 2, 2013

MEMORANDUM FOR: The Honorable Rafael Borras
Under Secretary of Management
Department of Homeland Security

FROM: Charles K. Edwards
Deputy Inspector General

SUBJECT: *Reducing Over-classification of DHS' National Security Information*

Attached for your information is our final report, *Reducing Over-classification of DHS' National Security Information.* We incorporated the formal comments from the Department in the final report.

The report contains two recommendations to aid the efforts of the Office of Management and the Office of the Chief Security Officer to enhance the program's overall effectiveness. The Department concurred with both recommendations and, based on information provided in the Department's response, we consider all recommendations to be open and resolved.

As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Please email a signed PDF copy of all responses and closeout requests to the Office of Inspections at OIGInspectionsFollowup@oig.dhs.gov. Until your response is received and evaluated, the recommendations will be considered resolved and open.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Deborah L. Outten-Mills, Acting Inspector General for Inspections, at (202) 254-4015, or Anthony D. Crawford, Intelligence Officer, at (202) 254-4027.

Attachment

Table of Contents

Appendixes

Abbreviations

ASD	Administrative Security Division
CAPCO	Controlled Access Program Coordination Office
CBT	computer-based training
CCSO	Component Chief Security Officer
CFR	Code of Federal Regulations
CIAO	Classified Information Advisory Officer
CMT	Classification Management Tool
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
E.O.	Executive Order
FCGR	Fundamental Classification Guidance Review
I&A	Office of Intelligence and Analysis
IC	intelligence community
ICD	Intelligence Community Directive
IPAG	Intelligence Policy Advisory Group
ISOO	Information Security Oversight Office
LMS	Learning Management System
NPPD	National Protection and Programs Directorate
NSI	national security information
OCA	original classification authority
OCSO	Office of the Chief Security Officer
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
P.L.	Public Law
SCG	security classification guide
SCR	security compliance review
S&T	Science and Technology Directorate
STWG	Security Training Working Group
USCG	U.S. Coast Guard
USSS	United States Secret Service

Executive Summary

The Department of Homeland Security (DHS) creates, receives, handles, and stores classified information as part of its homeland security, emergency response, and continuity missions. As creators and users of classified information, DHS is responsible for both implementing national policies and establishing departmental policies, to ensure that such information is adequately safeguarded when necessary and appropriately shared whenever possible. With proper classification of intelligence products, DHS can share more information with State, local, and tribal entities, as well as the private sector.

The *Reducing Over-Classification Act* of October 2010 (Public Law 111-258) requires the DHS Secretary to develop a strategy to prevent the over-classification and promote the sharing of homeland security and other information. This is the first of two reviews we are mandated to conduct under this act.

Specifically, we assessed the overall state of the DHS national security information program and reviewed 13 DHS components to determine whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered. We also identified policies, procedures, rules, regulations, and management practices that may be contributing to persistent misclassification. We coordinated with other Offices of Inspector General and the Information Security Oversight Office of the National Archives and Records Administration to ensure that our review's evaluations followed a consistent methodology that allowed for cross-agency comparisons.

As a result of our review, we determined that DHS has adopted and successfully implemented all policies and procedures required by applicable Federal regulations and intelligence community directives. Through implementing Office of the Chief Security Officer's policies and procedures, DHS has a strong program that should lead to better communication and sharing of intelligence throughout the Federal Government and with State, local, and tribal entities, as well as private sector partners. However, the Department's program can be strengthened by deploying a new classification management tool after testing, and by capturing all classified holdings better. We are making two recommendations that when implemented will improve the Department's overall management of its classification processes. The Department concurred with both recommendations.

Background

Since 1940, executive orders have directed government-wide classification standards and procedures. On December 29, 2009, President Obama signed Executive Order (E.O.) 13526, *Classified National Security Information* (order), which establishes the current principles, policies, and procedures for classification. The order prescribes a uniform system to classify, safeguard, and declassify national security information (NSI). According to the order, the Nation's progress depends on the free flow of information within the Federal Government and to the public. Protecting information critical to national security and demonstrating a commitment to open government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities. Misclassification of national security information impedes effective information sharing and may provide adversaries with information that could harm the United States and its allies and cause millions of dollars in avoidable administrative costs.

According to the order, information that is determined to require protection from unauthorized disclosure in order to prevent damage to national security must be marked appropriately to indicate its classification. The expected damage to national security determines the classification level, as follows:

- Top Secret – applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to national security that the original classification authority is able to identify or describe.
- Secret – applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security that the original classification authority is able to identify or describe.
- Confidential – applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to national security that the original classification authority is able to identify or describe.

Also according to the order, no other terms are to be used to identify U.S. classified information, except as otherwise provided by statute. If significant doubt exists about the need to classify or the appropriate level of classification, the information shall not be classified or shall be classified at the lower level.

Only original classification authorities (OCAs) authorized in writing by the President, the Vice President, or agency heads or other officials designated by the President may originally classify information. Prior to originally classifying information, OCAs must be trained on proper classification, and they must be trained at least once per year

thereafter. To make an original classification decision, an OCA must determine whether the information meets the following standards for classification:

- The information is owned, controlled, or produced by or for the Federal Government;
- The information falls within one or more of the eight categories (reasons for classification) of information described in Section 1.4 of E.O. 13526; and
- The unauthorized disclosure of the information reasonably could be expected to result in damage to national security that the OCA is able to identify or describe.

Original classification precedes all other aspects of the security classification system, including derivative classification, safeguarding, and declassification.

As an OCA, so delegated by the President, the DHS Secretary has the authority to classify information pursuant to classification standards cited in the order, and to further delegate such authority to additional DHS officials. The Secretary has delegated classification authority to designated subordinate officials who need to exercise this authority.

Derivative classification means incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material according to classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Personnel who apply derivative classification markings must be trained to apply the principles of E.O. 13526 prior to derivatively classifying information and at least once every 2 years thereafter. Information may be derivatively classified from a source document or documents, or by using a classification guide.

Authorized holders of information (including holders outside the classifying organization) who believe that a classification is improper are encouraged and expected to challenge the classification status of the information.

Federal Government departments and agencies that create or hold classified information are responsible for its proper management. Classification management includes developing classification guides with OCA instructions for derivative classifiers that identify information on specific subjects that must be classified, as well as the level and duration of classification. Applying standard classification and control markings is one of the most effective ways to uniformly and consistently identify and protect

classified information. Effective program management also includes comprehensive mandatory training for classifiers and a comprehensive self-inspection program.

Federal Government departments and agencies also may have systems of restrictive caveats that can be added to documents. These restrictions are not classifications; rather, they limit the dissemination of information.

Over-classification is defined as classifying information that does not meet one or more of the standards necessary for classification under E.O. 13526. Over-classification results in the unnecessary protection of information that is not sensitive, and inhibits the sharing of critical information.

The *Reducing Over-Classification Act* of October 2010 requires the DHS Secretary to develop a strategy to prevent the over-classification and promote the sharing of homeland security and other information. This is the first of two reviews the act mandates. Specifically, we assessed whether DHS Headquarters and its components and offices have adopted, followed, and effectively administered applicable classification policies, procedures, rules, and regulations; identified policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification; and coordinated with other Inspectors General and the Information Security Oversight Office (ISOO) to ensure that our evaluations followed a consistent methodology that allowed for cross-agency comparisons.[1]

We reviewed the DHS Office of the Chief Security Officer (OCSO) and the following 13 DHS components that are able to handle, produce, and classify information:

Domestic Nuclear Detection Office (DNDO)
Federal Emergency Management Agency
Federal Law Enforcement Training Center
National Protection and Programs Directorate (NPPD)
Office of Inspector General (OIG)
Office of Intelligence and Analysis (I&A)
Science and Technology Directorate (S&T)
Transportation Security Administration
U.S. Citizenship and Immigration Services
U.S. Coast Guard (USCG)
U.S. Customs and Border Protection
U.S. Immigration and Customs Enforcement

[1] ISOO, a component of the National Archives and Records Administration, is responsible to the President for policy and oversight of the government-wide security classification system and the National Industrial Security Program. ISOO receives policy and program guidance from the National Security Council.

United States Secret Service (USSS)

Results of Review

This is the first of two reports required by Section 6(b) of the *Reducing Over-Classification Act*, which mandates that OIGs of Federal departments and agencies with officers or employees authorized to make original classifications (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within the department or agency; and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material. The act was designed to prevent over-classification and over-compartmentalization of information, while promoting the sharing and declassifying of it, as prescribed by Federal guidelines. In this report, we address areas of classification management and control marking programs. For the second report, which is due on September 30, 2016, we will focus on follow-up efforts to this report's recommendations.

In assessing the DHS program, we reviewed the classification management and control marking programs of the OCSO and 13 components to ensure that they have the necessary resources to implement programs effectively, records systems are designed and maintained to optimize appropriate sharing and safeguarding of classified information, and senior agency officials are designated to direct and administer programs.

DHS OCSO and its components have implemented, managed, and provided oversight effectively for a classified National Security Information program as outlined in E.O. 13526, *Classified National Security Information*; Public Law (P.L.) 111-258, *Reducing Over-Classification Act*; 32 Code of Federal Regulations (CFR), Part 2001; and Intelligence Community Directive (ICD) Number 710, *Classification and Control Markings System*, September 2009. Specifically, the OCSO has created and implemented policies and procedures that established a firm foundation for DHS. DHS has met the program management, classification management, security education and training, and self-inspections requirements as specified in E.O. 13526 and 32 CFR, Part 2001. The Department has also fulfilled the requirements for classification guides, as well as original and derivative classification authorities, and how to challenge incorrect classifications.

However, we identified areas where improvements are needed. For example, 59 of the 372 DHS documents we reviewed contained declassification, sourcing, and marking errors. Also, all Classification Management Tools (CMTs) were outdated, which led to

declassification errors. Errors could lead to documents not being shared or being shared with personnel not cleared to handle them. DHS could also improve its collection of component information on classified holdings and its original and derivative classification decisions.

General Program Management

Program Management Overview

The Administrative Security Division (ASD) in the OCSO of the Management Directorate directs and implements DHS' National Security Information Program. Under the authority of the E.O., the Secretary has appointed the DHS Chief Security Officer as the Department's senior agency official with responsibility for ensuring the program is in compliance with all Federal directives, policies, and laws, and is adopted and implemented by all DHS components that handle and classify national security information.

ASD and senior management create and implement classification policies for all DHS components and for all State, local, tribal, and private sector entities as the policies relate to Homeland Security. Senior management direction has enabled ASD to instruct DHS components and ensure that the Department is in compliance with all policies. Coordination among senior management, the OCSO, and Component Chief Security Officers (CCSOs) in components and offices has enhanced the proper classification, declassification, handling, and safeguarding of information. Senior management is apprised of all security policy changes, and reviews all reported security violations and self-inspection results.

DHS Instruction 121-01-011 specifies the procedures and requirements for classification challenges, sanctions, self-inspections, reporting and definitions, and security training. Eight of the 13 components and offices that we reviewed have CCSOs who oversee their respective programs and implement changes to instructions from the OCSO. The other five Headquarters offices—DNDO, NPPD, OIG, I&A, and S&T—have internal security staff and, with the exception of OIG, OCSO security support embedded within the offices to assist with implementation and oversight of security matters.

DHS CCSO's and other invited officials meet once a quarter to discuss security issues and policy changes. DHS uses various working groups, such as the group that creates instructional documents for the NSI program. I&A and the USCG also attend the Classification Management Intelligence Working Group and Classification Management Tools Working Group as members of the Intelligence

Community (IC). These working groups have led to improvements in security classification guides and training, and have enhanced the Department's classification culture.

Security Program Management

According to ISOO's October 2008 evaluation of DHS' information security program, DHS' oversight and consistent implementation of the program complied with applicable policies and regulations. However, ISOO identified weaknesses in classification markings, self-inspections, and personnel performance plans.

This section will focus on the core issues of security program management, including DHS' responsibilities in implementing its security program in compliance with E.O. 13526. These include the agency head's responsibility to support the program and the responsibility of the senior agency official designated by the agency head to direct and administer the program. DHS has an appointed senior agency official to direct and administer the program, whose responsibilities include the following:

- Overseeing the program established under E.O. 13526;
- Issuing implementing regulations;
- Establishing and maintaining security education and training programs;
- Establishing and maintaining an ongoing self-inspection program;
- Ensuring that the designation and management of classified information is included as a critical rating element for OCAs, security managers or security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information, including those who apply derivative classification markings; and
- Establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and providing guidance to personnel on proper classification, as needed.

Classification Management and Control Marking Policies

DHS has adopted and implemented effectively all critical elements required for applicable classification policies, procedures, rules, and regulations in E.O. 13526 and 32 CFR, Part 2001. Subsequent to the issuance of the E.O. in 2009, DHS revised and consolidated existing administrative information security policies

into a single Department-wide instruction that reflected and effectively implemented changes resulting from publication of the E.O.

As required by the *Reducing Over-Classification Act*, DHS appointed a Classified Information Advisory Officer (CIAO) to assist in sharing information with State, local, and tribal entities; law enforcement; and the private sector.[2] DHS appointed a CIAO in November 2010 and submitted written notification to the U.S. Senate Homeland Security and Governmental Affairs Committee and House Committee on Homeland Security. The CIAO's duties include those described in the act and E.O. 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities,* and the implementing directive for E.O. 13549 approved by the Secretary in February 2012. Before passage of the act, DHS made efforts to educate State and local partners in the identification, classification, safeguarding, and handling of classified information, and it continues to do so.

ASD's DHS Instruction 121-01-011, *The Department of Homeland Security Administrative Security Program,* of April 2011, establishes procedures, program responsibilities, minimum standards, and reporting protocols for DHS. The instruction cites E.O. 13526 and 32 CFR, Part 2001 for authorization of its NSI program. DHS also follows all Controlled Access Program Coordination Office (CAPCO) instructions for classified markings in ICD 710, where required.

DHS Instruction 121-01-011 does not address special access programs, which are governed by DHS Directive 140-04, *Special Access Program Management,* and DHS Instruction 140-04-001, *Special Access Program Implementation*. These are reviewed annually in compliance with E.O. 13526.

All 13 DHS components and offices that we reviewed have adopted and implemented the policies and procedures required in DHS Instruction 121-01-011. CCSOs agree that the DHS instructions provide the necessary information for efficient and effective security programs. Only USSS and the USCG have developed supplemental instructions related to their specific security programs; the Federal Law Enforcement Training Center is developing a security policy as a subset to the DHS instruction.

DHS has published 6 CFR, Part 7, which covers DHS-classified NSI and is currently awaiting Office of General Counsel approval for an updated version to be in compliance with E.O. 13526.

[2] P.L. 111-258, *Reducing Over-Classification Act,* Section 4(a).

OCSO senior management stated that reducing over-classification is important, and has demonstrated the Department's successful adaptation and implementation of the security program established in E.O. 13526. DHS' commitment to ensuring that the security program is implemented effectively as established under this order is evident throughout the Department's components and offices.

Classification Management Tools

CMTs allow users to automatically apply classification markings to electronic documents. Not all DHS components are using CMTs, and where a CMT is used it has not been updated to reflect changes resulting from the publication of E.O. 13526. Thus, DHS' use of CMTs is not in complete compliance with E.O. 13526, and classifiers may be incorrectly classifying or declassifying information in their documents. We believe that the new CMT will reduce errors in classification and declassification and eliminate some current marking issues.

During our document review, we also identified a problem with using a specific declassification exemption called 50X1-HUM.[3] Documents that should have been marked 50X1-HUM were marked with either a numerical 50-year date or "25x1" and a 50-year date. This problem stems from current CMTs not allowing the use of 50X1-HUM as the proper classification.

In addition, in some components and offices, CMTs do not allow for changes to classification carried over from the source. Some CMTs also do not offer proper exemptions, which results in extended declassification dates, and do not prompt users to mark portions of the body of an email.

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 marks against the banner, ensuring marking consistency and more effective protection of national security.

DHS is currently testing a new CMT developed by the IC, which may be used for all DHS components with C-LAN access. The new CMT is in accordance with E.O.

[3] 50X1-HUM is a term used for an exemption to declassifying information after 50 years, which is the timeframe in E.O. 13526 and 32 CFR, Part 2001. It reflects a decision by the Interagency Security Classification Appeals Panel to classify information beyond 50 years.

13526; 32 CFR, Part 2001; and CAPCO guidance. DHS has adopted the IC format, but has also included specific caveats and security classifications guides (SCGs) for DHS missions. The tool is still in its pilot stage; therefore, only a few select employees from nine components have access to it. The new CMT provides all appropriate exemptions, allowing for a proper declassification date, and it enables users to change the classification levels of emails to reflect new ones; it also prompts users to mark portions of documents.

Challenging Classification

In accordance with E.O. 13526, DHS Instruction 121-01-011 includes procedures for informally and formally challenging the classification status of information, noting that all DHS employees and contractors may challenge any classification that they believe might be over- or under-classified.

DHS senior management we interviewed believes that challenging the classification status of information is part of an employee's job. When asked, 90 out of 100 DHS derivative classifier interviewees said that they believed offering incentives may lead to unnecessary challenges, and challenges will be raised not in the spirit of reducing classification but for incentive reasons.

An authorized holder of classified information is not prohibited from informally questioning the classification of information through direct and informal contact with the classifier. All persons interviewed said they preferred informal questioning for handling classification challenges, but they recognized this does not always solve the issue and a formal process may be necessary.

The DHS instruction includes a process for formal challenges. 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. The individual submitting the challenge has a right to appeal the decision to the Interagency Security Classification Appeals Panel established by Section 5.3 of E.O. 13526 and/or the DHS Chief Security Officer acting as the senior agency official, who convenes a DHS Classification Appeals Panel. Individuals who challenge classifications are not subject to retribution. ASD honors a challenger's request for anonymity and serves as his or her agent in processing the challenge. DHS has a secure capability to receive information, allegations, or classification challenges.

ASD and CCSOs should continue communicating to employees the importance of challenging the classification status of information to both protect and promote the sharing of information.

Security Violations and Sanctions

We determined that DHS Instruction 121-01-011 is in compliance with E.O. 13526 as it relates to security violations and sanctions. The DHS instruction includes a process for handling security violations and sanctioning violators.

According to the E.O., the agency head, senior agency official, or other supervisory official should, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this E.O. Incidents involving the mishandling or compromise of classified information must be reported promptly to the servicing security official and investigated thoroughly to determine the cause. Security officials must assess and mitigate potential damage, and implement measures to prevent recurrence. The agency head or senior agency official must take appropriate and prompt corrective action and notify the Director of ISOO when certain violations occur.

The DHS instruction also includes information on reporting a security incident, reportable security incidents, security inquiries, and what constitutes a formal investigation. It covers incidents involving classified information within information technology systems, security violations and infractions in foreign countries, other agency security violations and infractions, and sanctions.

To conduct a proper inquiry or investigation and respond to possible security incidents, DHS components and offices gather and include key information, such as names, dates, causes, and mitigation efforts in the Security Inquiry Reports. Once completed, a report is forwarded to the official(s) with jurisdiction over the component or office where the security incident occurred, as well as the person(s) involved, for further action as appropriate. A copy of the report is also forwarded to the servicing personnel security office, where it is filed within the personnel security folder of the individual(s) found to be culpable for commission of the incident.

According to the instruction, sanctions may include verbal or written counseling, reprimand, suspension from duty with or without pay, removal, or revocation of access to classified information, termination of classification authority, or criminal penalties. Administrative sanctions are assessed in accordance with the policies, procedures, and practices established by the human capital office in the

component or office. Security clearances must be revoked or suspended in accordance with applicable E.O.s and Office of the Director of National Intelligence (ODNI) policies and regulations.

When a proposed sanction associated with the unauthorized disclosure of classified information exceeds a reprimand, the matter must be coordinated with the DHS Office of General Counsel. Further, if there is an allegation that a criminal violation has occurred, the matter is coordinated with the Office of General Counsel and the Department of Justice.

Recommendation

We recommend that the Office of Management:

Recommendation #1: Ensure that DHS fully deploys the new Classification Management Tool to all DHS components and offices when pilot testing is completed.

Management Comments and OIG Analysis

We evaluated the Department's written response and have made changes to the report where we deemed appropriate. A summary of the Department's written response to the report recommendations and our analysis of the response follows each recommendation. A copy of DHS' response, in its entirety, is included as appendix C.

In addition, we received technical comments from the Department and incorporated these into the report where appropriate. DHS concurred with all recommendations in the report. We appreciate the comments and contributions made by DHS.

Management Response: Office of Management officials concurred with recommendation 1. In its response, the Office of Management said that the CMT pilot phase of testing is being finalized, and the funded purchase request for DHS to procure the CMT is processing through the procurement system to create an interagency agreement with the owning agency to be completed within the coming weeks. The Office of the Chief Information Officer will proceed with full deployment of the tool to the top secret and secret networks. Concurrent with full deployment, OCSO will conduct initial individualized training essential to the successful deployment and use of the CMT. The Office of Management estimates a completion date of February 28, 2014.

OIG Analysis: We consider the Office of Management's actions responsive to the intent of Recommendation 1, which is resolved and open. This recommendation will remain open pending full deployment of CMT.

Original Classification Authority

We determined that the DHS Secretary, in accordance with Federal guidance, designated OCAs to determine the original classification of documents. We determined that the OCAs are following processes described in E.O. 13526 and 32 CFR, Part 2001 for making original classification decisions.

Original Classification Authority Designation

In accordance with Section 1.3 of E.O. 13526 and 32 CFR Section 2001.11, the DHS Secretary designates various DHS officials who are authorized to classify national security information. In DHS Delegation 8100, version 5, *Delegation of Original Classification Authority*, issued in June 2010, the DHS Secretary delegated original classification authority for Top Secret, Secret, and Confidential to 18 OCAs; 7 OCAs were delegated authority for Secret and Confidential. DHS reports OCA delegations to the Director of ISOO annually, as directed by Federal policies. Designating OCAs by position ensures clarity and continuity of classification responsibilities; if a person in a position delegated as an OCA cannot fulfill the duty or leaves the position, the successor inherits the duty and responsibilities of the OCA.

Original Classification Authority Program Training and Knowledge

All OCAs have received annual training as prescribed in E.O. 13526 and 32 CFR, Part 2001. At the time of this report, DNDO's OCA was scheduled for training. The training covers duties and responsibilities of an OCA and the proper application of classification markings. According to DHS Instruction 121-01-011, authority will be suspended for OCAs who fail to complete OCA training annually or in a timely manner.

The two OCAs we interviewed were knowledgeable about their duties and responsibilities in executing their mission. They were able to identify and describe the different types of damage to national security in cases of unauthorized disclosure of Top Secret, Secret, or Confidential information. The OCAs also understood that if their duties are not carried out as stated in E.O. 13526 or the CFR, they could be subjected to sanctions that include reprimand, suspension without pay, removal, loss of classification authority, loss or denial of

access to classified information, or other sanctions in accordance with applicable laws and Department regulations. Also, that their OCA authority may be suspended if they do not receive training in a timely manner.

We interviewed two OCAs that said they made original classification decisions within the past year. The original classification documents we reviewed were in accordance with Section 1.4 of E.O. 13526, which specifies the types of information that should be considered for classification.

Most DHS components and offices are consumers of intelligence information and rarely have to make original classification decisions. In fact, few DHS OCAs have made original classification decisions. Although OCAs may make few or no original classification decisions in a year, some have published and must maintain security classification guidance and OCAs must be available to address classification-related questions. As such, the current number of DHS OCAs is consistent with the need for OCAs as stipulated in E.O. 13526.

Original Classification and Dissemination of Control Marking Decisions

To communicate an original classification decision, the information to which the decision applies, the classification level, declassification instructions, and any other special instructions, security classification guides are written and approved by the OCA. SCGs provide requirements and standards for classifying information related to a department or agency's mission. According to E.O. 13526, information should be considered for classification if it covers specific categories, or if the compilation of related information meets the order's defined standards and criteria for classification and it falls under one or more of the categories of information listed in Section 1.4 of the order.

We determined that the eight SCGs we reviewed are in accordance with all policies, procedures, rules, and regulations. OCSO efforts for DHS components to write streamlined and uniform SCGs have led to a reduction of SCGs for the Department.

As of July 2012, DHS has 45 SCGs, down from 74 the previous year. The eight SCGs that we reviewed contained information related to the types, topics, reasons, levels, and duration of classifications, as described in E.O. 13526. All SCGs we reviewed were signed by an OCA delegated by the DHS Secretary. As per DHS Instructions, the OCSO maintains a master index of all DHS-published SCGs. OCSO initiates a review of the Department's SCGs at least every 5 years, which is in compliance with 32 CFR, Part 2001.

Derivative Classification and Dissemination of Control Marking Decisions

DHS is a vast consumer of intelligence information and the majority of DHS intelligence products are derivatively classified. Through interviews with 100 derivative classifiers department-wide, we determined that 95 of them are able to derivatively classify information properly, and have an overall understanding of the derivative classification process.

We determined that DHS Instruction 121-01-011 covers the use and inclusion of source materials and determining correct classification and declassification for derivative classifiers to make a decision. It also includes information on using technical documents or notes, foreign government information, and transmittal documents. Each section of the instruction describes the requirements for classification, as well as means of reducing over-classification, as specified in E.O. 13526 and 32 CFR, Part 2001.

According to the CCSOs and the personnel we interviewed, all had received training in the past 2 years and had received annual refresher training. They received classification training at the DHS Entry-on-Board course, through training by DHS security trainers and Special Security Officer trainers, online, through video teleconferencing, or via compact disks.

The derivative classifiers that we interviewed said that the required 2-year annual training for derivative classifiers and the annual refresher training are helpful in their classification duties. All individuals, except one, believed that training was adequate in teaching them how to make derivative classification decisions and how to apply classification markings properly. Eighty interviewees noted that they would like more hands-on training to ensure they could classify information properly.

All DHS derivative classifiers interviewed were able to define their responsibilities for derivative classification and the differences between derivative and original classification. They explained the key elements included in marking classified documents and handling caveats for their respective component and in compliance with CAPCO guidance.

All personnel knew how to determine declassification dates for documents derived from multiple sources or that carried forward multiple dates. Most determined that they would use a matrix approach to ensure they were capturing all dates and exemption categories.

When asked what derivative classifiers should do if they encountered information that they believed should be classified and is not, all answered that they would first secure the document to the level they think it should be classified. Next, they would contact the originating source to determine why it was not classified. If the originating source could not answer, they would contact their Senior Security Officer for clarification and to determine whether an OCA could classify the information.

The staff we interviewed knew whether their component or office had an OCA and SCGs. However, 15 of the 75 personnel whom we interviewed at components with SCGs had not used the guides because they have not seen them.

All persons interviewed knew and were trained on the process of formally or informally challenging a classification, but some stated that they would be reluctant to disagree with the originator's classification. They did not fear retribution from senior management, but they did not believe that they were experts in challenging classifications.

The derivative classifiers we interviewed believe that senior management and policies are sufficient to create, protect, and disseminate classified documents. The derivative classifiers stated that they had seen improvement in security practices, classifying, and marking of documents.

Security Self-Inspection Program

According to the 2008 ISOO On-site Review of DHS, its security compliance review (SCR) program, which includes the self-inspection program, was one of the weaker areas of the Department's NSI program. However, we determined that the security compliance review program, specifically the self-inspection program, is one of the strongest parts of the program now. Each DHS component and office that generates classified information is required to establish a self-inspection program. The self-inspection includes reviews of original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight, to ensure compliance with E.O. 13526 and 32 CFR, Part 2001. During self-inspections, components and offices examine classified products, email, and presentations for proper classifications and markings. We verified that the OCSO and the 13 components and offices we reviewed had conducted SCRs or self-inspections and sent their findings to senior leadership within the past 12 months.

ASD created and disseminates to the components a standardized checklist for their use in conducting a self-inspection once a year. Further, ASD conducts a compliance review of each component program once every 18 months. Component or office heads or designated Senior Security Officers may conduct unlimited self-inspections. The SCR team from ASD inspects every aspect of the NSI program and interviews personnel to gauge their understanding of policies and procedures in handling, safeguarding, and classifying information.

SCRs conducted by the SCR team or self-inspections by CCSOs include personal interviews with derivative classifiers to determine whether they are aware of their responsibilities for reducing over-classification and to determine their knowledge of proper markings. Part of each inspection is a classification review of a sample set of documents and a security check to determine whether proper security procedures are followed. Upon completion of the SCR or self-inspection, the results are compiled into a single report, which is presented to senior management. Reports are also sent to inspected areas so that necessary corrections can be made.

ASD provides its compliance review findings to component or office senior management and gives them a timeframe to respond with corrective measures. In accordance with E.O. 13526, ASD provides ISOO with an annual report reflecting the status of the DHS self-inspection and SCR programs.

Classified Document Review

We determined that DHS is doing a good job of applying classification to their documents as spelled out in the order and CFR. In our review, of the 372 classified documents, 59 or approximately 16 percent contained errors. For example, 23 documents had incorrect declassification dates and 14 were missing information on the classifier. Incorrect declassification dates could affect the use and sharing of information; not naming the classifier could call into question whether the individual had the proper authority to classify the document. Although most errors were minor and could have been avoided if classifiers were more precise, until DHS has a new CMT, these issues will likely continue.

Security Reporting

As required by E.O. 13526 and 32 CFR, Part 2001, DHS has provided all statistical reports to ISOO on classification activities, costs, fundamental classification guidance reviews, self-inspections, and security violations in a timely manner.

Fundamental Classification Guidance Review

The Fundamental Classification Guidance Review (FCGR) serves as a 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 classification guides also ensure standardized classification within and across Federal agencies. Overall, our review shows that DHS is streamlining classification guidance and more clearly identifying categories of what can be released and what needs to remain classified.

In 2012, DHS conducted a FCGR of all 74 of its existing SCGs and reported the results to ISOO in July 2012. Of the 74 SCGs, 45 were revised, revalidated, and reissued; 16 were canceled; 11 were merged or absorbed into other guides; and 2 were transferred to other agencies. The 45 SCGs equated to a 39 percent reduction. Additionally, the DHS publications *Security Classification Guides – A Guide for Writing a DHS Security Classification Guide* and *Original Classification – A Guide for Original Classification Authorities* were revised and reissued to ensure consistency with and reflect changes resulting from the publication of E.O. 13526.

Classification Statistics Report

Although DHS reports security classification program statistics to ISOO as required by E.O. 13526 and 32 CFR, Part 2001, these statistics may not be accurate. DHS captures this classification information on the SF 311 *Agency Security Classification Management Program Data* form. Each DHS component and office compiles statistics and submits a single SF 311 form; the OCSO then compiles the statistics into one overall DHS report. Because of the increased use of the electronic environment to share and disseminate information, DHS includes in its statistics all classification decisions, regardless of media. Two CCSOs believe that the estimates on SF 311 forms may not be as accurate as they could be because, although the OCSO gives general directions on using the forms, each component and office has its own system for compiling statistics. By not having a standard way to collect statistics, DHS may not be able to report a true representation of its classified holdings or decisions.

Cost Estimate Report

As required by E.O. 13526, DHS submitted a cost estimate for classification-related activities in fiscal year 2012, SF 176, *Cost Estimate Report*, to ISOO in

February 2013. The report was based on information provided by DHS components and offices.

Recommendation

We recommend that the Office of the Chief Security Officer:

Recommendation #2: Create and implement a standard method for components to collect and report information for the SF 311 *Agency Security Classification Management Program Data* form.

Management Comments and OIG Analysis

Management Response: OCSO officials concurred with recommendation 2. In its response, OCSO said that it will explore the feasibility of creating a standardized method of accounting for classification decisions. OCSO stated that the accuracy and reliability of data reported through the SF 311 report is currently under discussion among reporting agencies within the executive branch, under the leadership of ISOO. OCSO will continue to support the ISOO in resolving reliability and accuracy issues of this reporting requirement. Pending any changes to the reporting criteria stipulated by ISOO, OCSO will coordinate with DHS Component Chief Security Officials to evaluate the feasibility of creating a standard DHS method for collecting the data. OCSO estimates a completion date of September 30, 2013.

OIG Analysis: We consider the Office of Management's actions responsive to the intent of recommendation 2, which is resolved and open. This recommendation will remain open pending documentation of new reporting criteria directed by ISOO or by OCSO for the Department.

Security Education and Training

DHS classification training has been developed in accordance with E.O. 13526 and 32 CFR, Part 2001. The ASD Security Training Branch leads a working group that includes attendees from each component and office, to create standardized training for the entire Department.

The DHS Security Education and Training Awareness program encompasses initial training, annual refresher training, and specialized training for OCAs and those who apply derivative classification markings, as well as termination briefings, designed to:

- Ensure that all employees who create, process, or handle classified information have a satisfactory knowledge and understanding of classification, safeguarding, and declassification policies and procedures;
- Increase uniformity in the conduct of agency security education and training programs; and
- Reduce instances of over-classification or improper classification, improper safeguarding, and inappropriate or inadequate declassification practices.

The Security Training Branch has created, implemented, and conducted adequate original and derivative classification training that is up-to-date and in compliance with E.O. 13526 and 32 CFR, Part 2001. According to training management personnel we interviewed, derivative training is accessible and held more frequently than initially indicated by component and office employees we interviewed. During compliance reviews, ISOO has commended DHS training management for its successful work for conducting and implementing training. The only inhibiting factor is the shortage of staff; however, the office has been able to disseminate training to all domestic DHS components and offices and to international offices.

The Security Training Branch conducts derivative and original classification training, but DHS also has "train the trainer" programs to assist CCSOs in training to their employees. In addition, the division offers a 2-hour in-person seminar for all DHS employees that can also be conducted as a webinar for personnel in the field or overseas and for senior management. Security Training Branch management pointed out that this training has reached every State and a large number of international posts, and that other Federal partner agencies use it to train personnel with clearances.

DHS has determined that any individuals who do or may perform a derivative classification action and individuals with access to classified systems shall be considered derivative classifiers and as such are mandated to attend derivative classifier training. Some components train all security clearance holders and some train only those needing access to C-LAN or the Homeland Secure Data Network classified data systems.

The Security Training Branch chairs the Security Training Working Group (STWG), which is comprised of security personnel from each component and various other security personnel. The STWG has standardized the derivative classification training department-wide. The training is now given in three venues; instructor-led (in person), Webinar (a combination of personnel use their computers to connect to the Homeland Security Information Network and a

phone bridge), and computer-based training (CBT). The CBT was developed by the Security Training Branch and USSS and met 508 compliance standards, which are federally mandated for creating accessible content for people that use assistive technologies.

The CBT was disseminated to the components to load on their Learning Management Systems (LMS) to provide training. The CBT was able to be loaded onto the USSS LMS with no USSS 508 compliance issues; however, the CBT was not able to be loaded onto headquarters LMS due to not meeting headquarters 508 compliance standards. DHS personnel can still load the CBT compact disk on their desktop computers to receive the training.

Security Training Branch personnel stated that Section 508 compliance standards for component LMS seem to be less stringent than those for the headquarters LMS "DHScovery." Training management would recommend that a section be dedicated to creating 508-compliant software training agency-wide, which would assist in more efficient, internal training software development. The derivative training is recorded in the Information Security Management System for all DHS personnel who receive the training and additionally in DHScovery for Federal headquarters personnel. All components also track completion of their employees in their respective training management systems.

Intelligence Community Cross-cutting Issues

I&A and the USCG are the DHS representatives to the IC, and we determined that there are no major issues with the IC as it relates to classification management policies and procedures. The only issue our IC members may have is with the possible single IC classification guide described in the *Intelligence Community Classification Guidance Findings and Recommendations Report* of January 2008, which included recommendations to move the IC toward common guidelines. DHS IC members believe that a single classification guide will have to take into account the different missions of IC members and unique access to sources and methods. DHS IC components believe the most significant benefit of a single classification guide would be the standardization of classification that transcends IC elements and is consistent and uniform.[4]

[4] ODNI has an ongoing effort to create a single classification guide that would standardize the framework of all guides, provide standard definitions for the concepts behind information that needs to be protected, and describe damage to national security.

I&A and the USCG maintain websites that provide access to electronic versions of ODNI updated policies and manuals. Personnel with the proper security clearances and a need to know have access to all policies and manuals via the C-LAN and the secret network. DHS has received all current and updated versions of ODNI and CAPCO policies through the Intelligence Policy Advisory Group (IPAG). The IPAG affords DHS the opportunity to provide feedback concerning DHS equities on all ODNI draft policies.

I&A and USCG IC representatives believe that the continuance of establishing and maintaining standard classification markings and formats that are consistent with national policies and the statutory missions of IC members will enhance information protection and dissemination.

Appendix A
Objectives, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This review was included in the *OIG Fiscal Year 2013 Annual Performance Plan*. Our objectives were to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within DHS and to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material.

We conducted our fieldwork from September 2012 to February 2013 and interviewed security managers and original and derivative classifiers; we reviewed documents from DHS headquarters and 13 components and offices.

We conducted this review under the authority of the *Inspector General Act of 1978*, as amended, and according to the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B
Recommendations

We recommend that the Office of Management:

Recommendation #1: Ensure that DHS fully deploys the new Classification Management Tool to all DHS components and offices when pilot testing is completed.

We recommend that the Office of the Chief Security Officer:

Recommendation #2: Create and implement a standard method for components to collect and report information for the SF 311 *Agency Security Classification Management Program Data* form.

Appendix C
Management Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 28, 2013

MEMORANDUM FOR: Charles K. Edwards
Deputy Inspector General
Office of Inspector General

FROM: Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

SUBJECT: OIG Draft Report, "Reducing Over-classification of DHS National Security Information" (Project No. 12-161-ISP)

Thank you for the opportunity to review and comment on this draft report. The U.S Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG's) work in planning and conducting its review and issuing this report.

The Department is pleased to note the OIG "determined that DHS has adopted and successfully implemented all policies and procedures required by applicable Federal regulations and intelligence community directives." We also appreciate OIG's recognition that the DHS Office of the Chief Security Officer (OCSO), within the Management Directorate, and DHS components have "effectively implemented, managed, and provided oversight for a classified National Security information program." DHS leadership remains committed to maintaining a vital, robust, credible, and proactive program for the administration and management of programs associated with the protection of classified and sensitive but unclassified information.

The draft report contained two recommendations with which the Department concurs. Specifically, OIG recommended:

Recommendation 1: That the DHS Office of Management ensure that DHS fully deploys the new Classification Management Tool to all DHS components and offices when pilot testing is completed.

Response: Concur. DHS Office of Intelligence and Analysis (I&A), through the National Security Systems–Joint Program Management Office (NSS-JPMO), and implemented by the Enterprise Networked Support Services of Enterprise Services Division of the DHS Office of the Chief Information Officer's (OCIO) IT Services Office, is finalizing the pilot phase of testing the Classification Management Tool (CMT). The CMT is a standardized automated marking tool created for use throughout the Intelligence Community. The funded purchase request for DHS to procure the CMT is making its way through the procurement system to create an inter-agency agreement with the owning agency and is expected to be completed within the coming weeks. Upon receipt of payment, OCIO will proceed with full deployment of the tool to the Homeland Secure

Data Network (HSDN)[1] and C-LAN[2] networks. Concurrent with full deployment and for a period of time thereafter, OCSO will also conduct initial individualized training essential to the successful deployment and use of the tool. Estimated Completion Date (ECD): February 28, 2014.

Recommendation 2: OIG also recommended that the Office of the Chief Security Officer create and implement a standard method for components to collect and report information for the SF 311 *Agency Security Classification Management Program Data* form.

Response: Concur. A standardized method of accounting for classification decisions may increase the accuracy and reliability of the final count provided to the Information Security Oversight Office (ISOO) as part of the annual reporting requirement, and, OCSO will explore the feasibility of creating such a standard. However, the accuracy and reliability of data reported through the SF 311 report is a matter currently under discussion amongst reporting agencies within the executive branch under the leadership of ISOO. The purpose of the discussion is to assess and re-evaluate the methods and criteria for collecting the data, particularly as it relates to classification decisions made and classified information processed within an electronic environment. OCSO will continue to support the ISOO in its efforts to resolve long-standing issues associated with the reliability and accuracy of this important reporting requirement and will follow their lead in the publication of any subsequent policy or guidance. Pending any changes to the reporting criteria stipulated by ISOO, OCSO will, in coordination with DHS Component Security Officials, evaluate the feasibility of creating a standard DHS method for collecting the data. ECD: September 30, 2013.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously submitted under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

[1] The HSDN is a classified wide-area network utilized by the Department, the Components, and other partners.
[2] The C-LAN is DHS's top secret network.

Appendix D
Document Review Results

OFFICE OF INSPECTOR GENERAL-OFFICE OF INSPECTIONS
CLASSIFIED DOCUMENT REVIEW RESULTS
U.S. DEPARTMENT OF HOMELAND SECURITY

LEVEL OF CLASSIFICATION	
Top Secret	60
Sensitive Compartmented Information	4
Secret	265
Confidential	43
TOTAL	**372**
TYPE OF DOCUMENT	
Cable/Message	66
Memo/Letter	14
Electronic Media/Email/Slide Presentations	64
Reports	121
Other (Intelligence Assessments and Notes, Briefings, Issue Papers, Talking Points)	107
TOTAL	**372**
BASIS FOR CLASSIFICATION	
Classification Guide	80
Multiple Sources	215
Single Source/Other	77
TOTAL	**372**
DURATION OF CLASSIFICATION	
Declassification less than 10 years	0
Declassification 10 years	30
Declassification >10 years, <25 years	69
Declassification 25 years	101
25X1 – 25X9	22
50X1 – HUM or 50X2 – WMD	114
Source Marked X1 – X8 (valid use)	1
Invalid Use of X1- X8	0
Other Invalid Marking	18
Not Indicated	17
TOTAL	**372**
DISCREPANCIES	
Declassification	23
Unknown Basis for Classification/“Derived From” Line	4

"Classified By" Line- Derivative Classification	14
Portion Marking	3
Multiple Sources Not Listed	7
Marking	4
Original/Derivative	0
"Reason" Line	2
Duration	2
TOTAL	**59**

Appendix E
Major Contributors to This Report

Deborah L. Outten-Mills, Acting Assistant Inspector General for Inspections
Anthony D. Crawford, Team Lead, Intelligence Officer
Ryan P. Cassidy, Program Analyst

Appendix F
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Management Liaison
Acting Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Committee on Homeland Security and Government Affairs
Select Committee on Intelligence
Committee on Homeland Security
Committee on Oversight and Government Reform
Permanent Select Committee on Intelligence

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.