Office of Inspector General
Audit Report

DOT DOES NOT FULLY COMPLY WITH REQUIREMENTS OF THE REDUCING OVER-CLASSIFICATION ACT

Department of Transportation

Report Number: FI-2013-136
Date Issued: September 19, 2013

Memorandum

U.S. Department of Transportation
Office of the Secretary
of Transportation
Office of Inspector General

Subject: ACTION: DOT Does Not Fully Comply with Requirements of the Reducing Over-Classification Act
Department of Transportation
Report Number FI-2013-136

Date: September 19, 2013

From: Louis King
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Assistant Secretary for Administration
Federal Aviation Administrator

During this era of heightened national security concerns, getting the right information to the right people requires accurate and accountable application of classification[1] standards. The Department of Transportation (DOT) and other Federal departments must first react internally to information regarding security threats, and then clearly communicate the status and implications of the threats to stakeholders. As the 9/11 Commission observed, the over-classification[2] of information interferes with accurate information sharing, increases the cost of information security, and limits stakeholders and public access to information.

In 2010, Congress passed the Reducing Over-Classification Act.[3] The Act requires Federal agencies that classify information to administer programs promoting compliance with laws regarding the proper use of classification and to reduce over-classification. The Act also requires the inspectors general of departments

[1] The Federal Government deems that certain information is sensitive and requires secrecy based on national security. Classification is the act of assigning a level of sensitivity to this information. The Federal Government established three levels of classification: Top Secret, Secret and Confidential.

[2] Over-classification occurs when a document is assigned a level of classification that is higher than needed. For example, a document that requires a secret classification but is designated top secret would be considered over-classified.

[3] The Act, P. L. 111-258, requires the Secretary of Homeland Security to develop a strategy to prevent the over-classification of homeland security and other information and to promote the sharing of unclassified homeland security and other information.

authorized to make original classifications,[4] in consultation with the National Archives and Records Administration's Information Security Oversight Office (ISOO),[5] to conduct two evaluations of their departments' classification programs by September 30, 2016, with the initial evaluation due September 30, 2013. To meet this requirement, we conducted an audit to (1) determine whether DOT has implemented effective policies and procedures for classification of information that comply with Federal policy and regulations, and (2) identify any practices that may lead to continuous misclassification of information.

We conducted this review between January and September 2013 in accordance with generally accepted Government auditing standards. We interviewed Department officials and reviewed Federal and departmental policy and regulations. We reviewed a statistical sample of 49 secret and confidential documents from a universe of 248 that the Department produced during 2010, 2011, and 2012 to test compliance with regulations. See Exhibit A for more details on our scope and methodology.

RESULTS IN BRIEF

Not all DOT classification related policies and procedures are effective or comply with Federal requirements, including ISOO's regulation. Specifically, the Office of the Secretary of Transportation (OST) did not conduct inspections of all areas where classified information is processed and stored. It also did not effectively review document markings.[6] In our statistical sample of 49 of 248 products classified as Confidential or Secret we found 35 that were not correctly marked. Based on our findings, we estimate[7] that 180, or 72.4 percent, of the Department's Confidential and Secret products are marked incorrectly. DOT officials noted that ISOO and internal policies were not clear as to whether or not certain documents required marking. In addition, the statistics on the number of classified documents produced and inspections conducted that OST reported to the ISOO contained inconsistencies. For example, in 2011, FAA reported 33 self-inspections to OST, but OST reported only one FAA self-inspection to ISOO; however, in 2012, OST reported all 48 FAA self-inspections. Last, FAA has not updated its order on safeguarding classified national security information since March 13, 2006. Both DOT and FAA did not assign adequate resources to reporting and policy updating.

---

[4] Original classification authority refers to an individual authorized in writing, either by the President, the Vice President, or agency heads or other officials designated by the President, to classify information in the first instance. Derivative classification is the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the new material consistently with the classification markings that apply to the source information.

[5] ISOO is responsible to the President for policy and oversight of the Governmentwide security classification system.

[6] The Federal Government requires documents or other media containing classified information to be clearly identified or "marked." These markings should be conspicuous, and immediately apparent to alert holders of the classified information, among other things.

[7] Our estimate has a margin of error of +/- 10.3 percentage points at the 90 percent confidence level.

Without comprehensive self-inspections, adequate markings, accurate reporting, and up-to-date policies, the Department is at increased risk that documents will not be properly classified or sufficiently protected.

We could not reach a conclusion as to whether there are practices that lead to continuous misclassification. For our sample of 49 documents, we did not have the necessary security clearances to review the sources for 33, or 67 percent, of our sampled items.[8] However, we reviewed the remaining 16, or 33 percent, and did not find any instances of misclassification. The Department has requested these clearances from the appropriate agency. Upon receipt of the clearances, we will complete this work.

We are making a series of recommendations for improving DOT's oversight of its Classified National Security Information program, and its compliance with the Reducing Over-Classification Act and the ISOO regulation.

BACKGROUND

In December 2009, the President signed Executive Order 13526 (EO), which updated previous expectations regarding the uniform system for classifying, safeguarding, and declassifying national security information. The EO specifies requirements for Federal agencies that classify information, including details on identification and marking requirements. Each classified document must be marked at the top and bottom of each page with its classification level—Confidential, Secret, or Top Secret. A derivative document—which is classified because the source of its information is another classified document—must be marked with certain original source document information, including the identity of the individual that created the document and the date of declassification.

In 2010, the ISOO issued its regulation[9] implementing EO 13526. The rule establishes guidance to Federal agencies on original and derivative classification, including markings and safeguarding of documents, downgrading classification levels, declassification, and fundamental classification guidance reviews. The rule also calls for agencies to conduct regular reviews of agencies' original and derivative classification actions and the physical protection and storage of classified materials. The regulations also state that self-inspections should cover original and derivative classifications, safeguarding, security violations, security education and training, as well as management and oversight of the program.

[8] To access a classified document, an individual needs to possess a security clearance at the level of the classification of the document or higher. For example, to access a document classified as "secret" requires a secret or top secret clearance.

[9] 32 CFR Parts 2001 and 2003, Classified National Security Information.

OST oversees most of the Department's operating administrations' classified information security processes and is responsible for the self-inspection program. In its policy, DOT specifically delegates authority to FAA to administer its own program under OST's oversight. DOT's Assistant Secretary for Administration is designated as the Senior Agency Official for classification management.[10] DOT has three areas with dedicated space designed for secure storage of classified information.

The Department has eight officials with original classification authority for the Secret classification level, including the Secretary of Transportation, Deputy Secretary of Transportation, FAA Administrator, and Maritime Administrator.[11] OST and some operating administrations, including MARAD, and FAA, perform derivative classification up to the Top Secret level. From 2011 to 2012, the number of derivative products that DOT produced increased from 88 to 1737.[12] The Department expects similar numbers of derivative products in the future.

ISOO's regulation also describes requirements for agencies' annual reporting to ISOO. Each agency that creates or safeguards classified information must annually report to the Director of ISOO statistics related to its classification program, including the number of original and derivative documents produced, and the number of self-inspections completed. FAA collects statistics on its classified documents and reports them to OST. Subsequently, OST collects statistics from all DOT's operational administrations and reports them to the ISOO.

DOT'S POLICIES AND PROCEDURES ARE NOT SUFFICIENTLY EFFECTIVE TO ENSURE PROPER MARKING AND INSPECTIONS OF CLASSIFIED DOCUMENTS

DOT's policies and procedures are not sufficiently effective and do not fully comply with the EO and ISOO's regulations. Specifically, DOT's self inspection program does not provide adequate coverage of either documents or physical locations; many documents were not properly marked; the statistics that OST reports to ISOO contained inconsistencies; and FAA's policy had not been updated to comply with EO 13526.

DOT's Self-Inspection Program Lacks the Necessary Coverage

DOT's self-inspection procedures are not adequate and do not fully comply with the EO's requirements. In its annual inspections, OST only selectively reviews

[10] In accordance with 49 CFR Part 8.

[11] The other four original classification authorities are the Assistant Secretary for Administration, OST's Director of Security and Director of Intelligence, Security and Emergency Response (S-60), and FAA's Assistant Administrator for Security and Hazardous Materials.

[12] Due primarily to FAA's expanded production of classified documents as a result of creating a threat intelligence organization in March 2012.

Operating Administrations for physical security infractions such as leaving security containers unlocked. In 2010, 2011, and 2012, OST did not review any of the 206 derivatively classified documents that S-60 and MARAD produced, and did not inspect the three primary locations for secure storage of classified information. DOT officials noted that they did not have sufficient resources to effectively conduct self-inspections. During our audit, we identified only one person assigned to this task.

OST Officials informed us that in 2013, OST began a more comprehensive self-inspection program that includes inspecting the Crisis Management Center, S-60 Intelligence Division, and MARAD's Command Center. Officials indicated that once that initial review is complete, they will share the results with us. Without comprehensive self-inspections, the Department does not know if documents are properly classified, and protected.

The Department's Classified Documents Were Not All Correctly Marked

We found that derivatively classified documents did not follow the control marking requirements. ISOO regulations require markings to include the identification of the person classifying the document, a listing of source materials, and the date or event for declassification. We reviewed 49 documents at the Confidential or Secret level, including one original classified document and 48 derivative ones, and found that 35 of the derivative documents were missing required markings. Based on our sample, we estimate that 180, or 72.4 percent, of 248 of the Department's Confidential or Secret products are marked incorrectly. Inadequately marked documents do not alert users to their sensitivity and increase the risk that documents will be compromised.

OST and FAA officials told us they did not properly mark these derivative products because they did not intend to release the documents outside the Department and some documents, such as briefings and threat analyses, were originally considered working papers—to be destroyed within 180 days—but operational issues required that the products be kept for a longer period. Furthermore, OST officials noted that ISOO or internal policies did not specify that electronic versions of briefings never intended for distribution or final intelligence production needed to be fully marked. OST and FAA also told us that they have since changed their processes to include briefings and threat analyses.

OST's Reports to ISOO Are Not Accurate

OST does not report accurate statistics to ISOO, and therefore, does not comply with ISOO's reporting requirements. We found inconsistencies between the Department's and FAA's statistics. For example, for 2011, FAA reported 33 self-inspections to OST, but OST reported only one FAA self-inspection to ISOO.

However, during 2012, DOT reported all 48 FAA self-inspections. Furthermore, while OST reported 1,900 derivative documents over the three year period, we found an additional 207 classified documents produced in the same period that OST did not report to ISOO.

We also found inconsistent applications of ISOO's requirements and definitions of what annual reports should include. For example, ISOO requires agencies to report original emails regarding derivative classification actions. However, some agency staff informed us that counting and reporting email as well as limitations on the email software they are required to use create an administrative burden on analysts and their ability to meet this requirement. As a result, they did not report emails.

Because of these inaccurate statistics, ISOO does not have a reliable basis for evaluating how well DOT safeguards classified materials, and cannot report reliable information on the status of the Governmentwide classified information program.

FAA's Policy Is Outdated

FAA's Order 1600.2E, Safeguarding Classified National Security Information (March 2006), has not been updated to address and comply with the EO as required by ISOO. For example, the existing order does not contain provisions relating to complying with ancillary marking requirements of derivative classifier identity and declassification date. FAA told us policy revisions were impacted due to organizational changes and resources. Lack of up-to-date policies increases the risk that documents will not be properly classified.

WE COULD NOT CONCLUDE WHETHER THERE ARE PRACTICES THAT LED TO CONTINUOUS MISCLASSIFICATION

Because the necessary security clearances are pending, we could not complete our review of supporting documentation and hence cannot definitively conclude at this time whether practices exist that would lead to continuous misclassification. Collectively, we possessed clearances that allowed us to review most levels of classified information. However, a significant portion of the information we needed to access to accomplish this objective was classified beyond our level of clearance. We worked with the Department to request the necessary clearance and access. The Department has processed our request and forwarded it to the responsible agency. We are awaiting the response from this agency. Within two months of receiving this response, if favorable, we will complete our review of supporting documentation to determine if there are practices that contribute to continuous misclassification.

Our sample of 49 classified documents included one originally classified document and 48 that contained information that was derived from classified sources. To determine whether these derivative documents were properly classified, we needed to review the source document used to create the derivative. We could not perform this review for 33 documents—which represents 67 percent of our sample—since they were derived from sources that were classified above our level of clearance. For the remaining 15 and the originally classified document, which represent 33 percent of our sample, we completed our review and found no instances of misclassification.

CONCLUSION

Classification of sensitive information is crucial to protect national security, transportation infrastructure and the public. Effective processes to identify, manage, and control classified information must be in place to make the information available only to those who need it, prevent over classification, and comply with Federal requirements. DOT has not sufficiently implemented policies or processes to conduct self-inspections, ensure proper classification markings, and accurately report classified information statistics to the ISOO. Until DOT takes additional actions to enforce compliance with Federal requirements, it will be unable to ensure that national security information is properly managed.

RECOMMENDATIONS

We recommend that DOT's Assistant Secretary for Administration:

1. Take steps to develop a more comprehensive self-inspection program that will include greater coverage of derivative documents and inspections of spaces dedicated to storage of classified documents (e.g. the Crisis Management Center).

2. Seek additional resources to complete comprehensive self inspections, and to prepare accurate reports to the National Archives and Records Administration's Information Security Oversight Office.

3. Take steps to implement policies and procedures that identify what documents need to be marked and how, and validate that these policies and procedures are consistently applied throughout the Department.

4. Establish a procedure and communicate to the OAs clear definitions and requirements for ensuring that annual reporting to the National Archives and Records Administration's Information Security Oversight Office is accurate and complete.

We recommend that the Federal Aviation Administrator, in consultation with the Assistant Secretary for Administration:

5. Update FAA's policy to conform to the requirements of EO 13526.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided DOT with our draft report on August 27, 2013, and received its response on September 12, 2013. DOT's response is included in its entirety in the appendix to this report. In its response, DOT concurred with all recommendations in the report, and requested that recommendation 4 be closed with the issuance of the report based on actions taken.

We agree, and have closed the recommendation.

ACTIONS REQUIRED

In accordance with follow-up provisions in Department of Transportation Order 8000.1C, we request, that DOT provide our office with documentation that its planned actions are complete within 10 days of their completion. Until we receive this information, we consider recommendations 1, 2, 3, and 5 are open until planned actions are completed and recommendation 4 is resolved and closed.

We appreciate the courtesies and cooperation of Department of Transportation and Federal Aviation Administration representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407 or Joann Adam, Program Director, at (202) 366-1488.

#

cc: DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted our work from January 2013 through September 2013 in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. For our second objective—identify practices that resulted in continuous misclassification—our scope was limited to Confidential and Secret level classified documents due to limitations of our security clearances. Because the documents we were able to review represented only 33 percent of our sample, we were unable to conclude as to whether such practices exist. Appropriate higher level security clearances were requested and are being processed by the appropriate Agency.

We reviewed DOT and its Operating Administrations' classified information, policies, procedures, rules, regulations, and management practices. We also interviewed officials with original and derivative classification authority and DOT officials responsible for managing the Classified National Security Information program.

We coordinated with other IG offices and with the Information Security Oversight Office via meetings and interviews. We followed the methodology prescribed in "A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the Reducing Over-Classification Act". The guide was prepared on behalf of the Council of Inspectors General on Integrity and Efficiency.

We received a list of 1,900 reported classified documents from OST. Because of the clearance level required for some of the documents or the low risk level, we only included 225 documents in our universe. We stratified the universe by organization, year, type of document, and clearance level and selected a simple random sample from each stratum for a total sample of 35 documents to review. While we were conducting our review, we also found 207 classified documents that were not on the reported list from OST. Once again, because of clearance level, we were only able to select a stratified sample of 14 from 23 of the 207 documents. In order to make our projections, we combined the two samples so that our final sample size was 49 classified documents out of a universe of 248 documents that were reported or found to be classified Confidential or Secret.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Joann Adam	Program Director
Lissette Mercado	Former Project Manager
LaKarla Lindsay	Senior Auditor
James Mullen	Information Technology Specialist
Meghann Noon	Auditor
Petra Swartzlander	Senior Statistician
Megha Joshipura	Statistician
Susan Neill	Writer-Editor

APPENDIX. AGENCY COMMENTS

U.S. Department of Transportation
Office of the Secretary of Transportation

Assistant Secretary for Administration

1200 New Jersey Avenue, SE
Washington, DC 20590

SEP 12 2013

MEMORANDUM TO: Louis King
Assistant Inspector General for Financial and Information Technology Audits

FROM: Brodi Fontenot

SUBJECT: Management Response to OIG Draft Report on the Department's Implementation of the Reducing Over-Classification Act

While the Office of Inspector General (OIG) review identified a number of issues predominantly with ancillary markings now required on classified documents, the OIG did not identify any specific instances of compromised classified information, or specific security vulnerabilities resulting from the types of issues identified.

Up until recently the Department has produced virtually no original classifications over the last 10 years. The vast majority of classification work is derivative and is used almost entirely for purely internal documents. Governmentwide requirements have evolved as a result of the latest executive order, particularly with regard to ancillary markings that are applied to documents to indicate who completed the original classification, when the information was classified, and when it should be declassified. Initially, there was some confusion government wide as to the applicability of this guidance to derivative classifications. Once these issues were clarified the Department immediately modified its processes and since that time has been ensuring that markings are clear and comply fully with the latest requirements.

RECOMMENDATIONS AND RESPONSES

Following are the recommendations included in the OIG draft report. The first four include responses from the Office of the Secretary, and the response to recommendation 5 is provided by FAA in consultation with OST in this consolidated Departmental response

Recommendation 1: Take steps to develop a more comprehensive self-inspection program that will include greater coverage of derivative documents and inspections of spaces dedicated to storage of classified documents.

Response: Concur. The Office of Security, working with other OST offices, has already taken steps to ensure the self-inspection program is as comprehensive as possible. For example, this year our self-inspections are on track to complete close to 100% of the Department, a rate not achieved in recent years. We have also acknowledged a need to include reviews of more classified documents than in the past as well as visits to high volume areas. The Office of Security will ensure these processes are captured in updated guidance by October 15, 2013

Recommendation 2: Seek additional resources to complete comprehensive self-inspections, and to prepare accurate reports to the National Archives and Records Administration's Information Security Oversight Office.

Response: Concur. OST will seek additional resources for performing the comprehensive self-inspections and reporting in fiscal year 2016. This action will be completed by February, 2014.

Recommendation 3: Take steps to implement policies and procedures that identify what documents need to be marked and how, and validate that these policies and procedures are consistently applied throughout the Department

Response: Concur. OST will re-verify that its existing policy and procedures for identifying what documents need to be marked and how are fully compliant with current Governmentwide requirements. Once confirmed, OST will reemphasize these procedures and the importance of adhering to them in a memorandum. Finally, we intend to convene a training/question and answer session with those individuals who perform the vast majority of marking in the Department to ensure the procedures are well understood. We plan to complete these actions by December 31, 2013.

Recommendation 4: Establish a procedure and communicate to the OAs clear definitions and requirements for ensuring that annual reporting to the National Archives and Records Administration's Information Security Oversight Office (ISOO) is accurate and complete.

Response: Concur. Based on discussions with the OIG during the course of its work, OST took immediate action to communicate to all DOT components clear definitions and requirements for ensuring annual reporting to ISOO is accurate and complete. These directions are included in a memorandum date February 13, 2013, provided separately to the OIG. Consequently we ask that this recommendation be considered closed upon issuance of the OIG report.

Recommendation 5: Update FAA's policy to conform to the requirements of EO 13526.

Response: Concur. While the vast majority of the requirements are included in FAA's 2006 Order, FAA recognized the need to provide full compliance with current requirements, and issued a draft revised order in April 2013. This draft order is proceeding through FAA's comprehensive clearance process, and is expected to be issued by December 31, 2013.