Office of Inspector General

Audit Report

IMPROVEMENTS INCREASE DOT'S COMPLIANCE WITH THE REDUCING OVER-CLASSIFICATION ACT

Department of Transportation

Report Number: FI-2017-006

Date Issued: November 7, 2016

Memorandum

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

Subject: **ACTION:** Improvements Increase DOT's Compliance With the Reducing Over-Classification Act
Department of Transportation
Report Number: FI-2017-006

Date: November 7, 2016

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

Reply to Attn. of: JA-20

To: Assistant Secretary for Administration
Federal Aviation Administrator

Information security is a top priority for the Department of Transportation (DOT) and other Federal agencies and requires accurate and accountable application of classification[1] standards. Such standards enable Federal departments to properly assess information regarding security threats and then clearly communicate the status and any implications to external stakeholders. As the 9/11 Commission observed, the overclassification[2] of information interferes with accurate information sharing, increases the cost of information security, and limits needed access to information.

In December 2009, the President signed an executive order (EO), updating requirements for Federal agencies for classifying, safeguarding, and declassifying national security information. In 2010, Congress passed the Reducing Over-Classification Act.[3] Among other things, the act requires inspectors general of departments authorized to make original classifications,[4] in consultation with the National Archives and Records Administration's (NARA) Information Security

[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] Overclassification 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 overclassified.
[3] Public Law No. 111-258 (2010).
[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.

Oversight Office (ISOO),[5] to conduct two evaluations of their departments' classification programs by September 30, 2016. We completed our initial evaluation on September 19, 2013, which found that DOT's policies and procedures were neither fully effective nor compliant with the EO and ISOO's regulations.[6] To meet the act's requirement for a second evaluation, we conducted an audit to (1) assess whether DOT has implemented policies and procedures to classify information effectively that comply with Federal policy and regulations and (2) identify any practices that may lead to persistent misclassification of information. As part of our review, we specifically examined the Federal Aviation Administration's (FAA) policies and practices since DOT policy delegates authority to FAA to administer its own classification program.

We conducted this review in accordance with generally accepted Government auditing standards. We interviewed Department officials and reviewed Federal and departmental policy and regulations. To test compliance with regulations, we reviewed a statistical sample of 40 out of 168 classified documents at the Office of the Secretary (OST) and 30 out of 708 classified documents at FAA that were produced from October 1, 2013, to June 30, 2015. The results of our statistical sample allowed us to project the extent of noncompliance with regulations. Exhibit A further details our scope and methodology.

RESULTS IN BRIEF

DOT has improved its compliance with Federal requirements for classification since our prior review through more comprehensive programs for employee training and agency self-inspections. However, some weaknesses persist at both OST and FAA. Of particular concern is FAA's outdated policy on safeguarding classified national security information—an issue we identified in 2013. FAA's reliance on a policy that has not been updated since 2006 has contributed to instances of noncompliance with more recent Federal requirements, such as derivative classifier identity. The EO required this policy be updated in 2010—almost 6 years ago. Management was unaware of several issues until we identified them. For example, none of the FAA employee performance plans we reviewed included handling of classified information as an evaluation item as required by the EO. In addition, both OST and FAA had document-marking errors.[7] For example, 7 of 30 documents in our FAA sample had incorrect declassification

[5] ISOO is responsible to the President for policy and oversight of the Government-wide security classification system. In 2010, ISOO issued its regulation (32 CFR Parts 2001 and 2003, Classified National Security Information) implementing Executive Order 13526.

[6] *DOT Does Not Fully Comply With Requirements of the Reducing Over-Classification Act* (OIG Report Number FI-2013-136), September 19, 2013. OIG reports are available at https://www.oig.dot.gov.

[7] 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. Each classified document must be marked at the top and bottom of each page with its classification level—Confidential, Secret, or Top Secret.

information. Finally, both OST and FAA did not retain the necessary classified information nondisclosure for several employees—6 of 36 tested at DOT and 50 of 125 tested at FAA. These were largely due to use of incorrect forms or recent changes in tracking systems or methods. Unless it fully addresses these issues, DOT risks that documents will not be properly classified or sufficiently protected.

We found few instances of overclassification—we estimate about 7.5 percent at OST and about 3.5 percent at FAA. In preparing documents, both OST and FAA use ISOO guidance and, aside from these exceptions, conformed to this guidance. We did note a practice that, while conforming to ISOO guidance, could result in overclassification of information in derivative documents.[8] This practice involves using sources at different classification levels in one paragraph. As required, the paragraph should be marked for the highest level of information in it. However, subsequent users may assume all information is at the same level and apply an incorrect, higher classification level when they extract information from the paragraph. We did not find any instances at DOT where this situation occurred and resulted in overclassification.

We are making seven new recommendations for improving DOT's compliance with the Reducing Over-Classification Act and the ISOO regulations. Exhibit B lists the status of the five recommendations made in 2013.

BACKGROUND

OST is required to oversee DOT Operating Administrations' (OA) classified information security processes and is responsible for the self-inspection program. OST collects statistics from all OAs and reports them to the ISOO. In its policy, DOT specifically delegates authority to FAA to administer its own program.

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.[9] DOT's Assistant Secretary for Administration is designated as the senior Agency official for classification management.[10] OST and FAA perform derivative classification up to the Top Secret level.

[8] 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.

[9] 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, and FAA's Associate Administrator for Security and Hazardous Materials Safety.

[10] In accordance with 49 CFR Part 8.

DOT and other Federal agencies must meet a number of requirements on proper application of document classification standards (see table 1).

Table 1. Select Federal Agency Classification Requirements

Purpose	*Requires*
2009 Executive Order 13526	
Updated requirements for classifying, safeguarding, declassifying, or changing classification levels of national security information	• Identification and marking for source and derivative documents • Identity of person who created document • Date of classification
2010 ISOO Regulation	
Established steps to implement requirements of EO 13526	• Regular agency self-inspections of original and derivative documents and storage/protection of classified materials • Self-inspections to include any security violations, security training and management steps, and program oversight • Agencies that create or safeguard classified information to report their self-inspection statistics annually to ISOO
2010 ROCA	
Promoted agencies' proper use of and/or reduction of classification	• Agencies to promote compliance with classification laws • DHS Secretary 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 • Inspectors general to evaluate their departments' classification programs twice by 9/30/16

Source: OIG analysis

DOT HAS IMPROVED ITS CLASSIFICATION PROGRAMS, BUT SOME WEAKNESSES REMAIN

Overall, DOT has improved its self-inspection programs and training. However, weaknesses exist in a number of areas. Of particular concern is FAA's outdated policy on safeguarding classified national security information. FAA also had included incomplete performance plans for users of classified information and incorrect self-inspection documents. Both OST and FAA had instances of document-marking errors and missing nondisclosure forms. These issues create the risk that DOT's documents will not be properly classified or sufficiently protected.

DOT Has Strengthened Some Key Controls

Due in part to our prior recommendations, DOT has strengthened a number of key controls. During our last audit, OST officials informed us that they were implementing a more comprehensive self-inspection program to include inspecting the Crisis Management Center, OST Intelligence Division, and the Maritime Administration's (MARAD) Command Center. During our current audit, we found this self-inspection program to be operational at DOT Headquarters.

OST has also taken strides to improve its training program. At the time of our review, all employees handling classified materials were provided initial and/or refresher training. In addition, OST offers training on derivative classification to employees with specialized needs in this area.

We also found adequate equipment labeling in Headquarters facilities. Such labeling includes, for example, placing a standard label on a printer that processes Secret material to let users know that that printer needs special handling. In a recent spot check of the Crisis Management Center, we observed, in addition to strict access controls, labels on computers, shredders, and other equipment.

Practices such as self-inspections, training, and equipment labels are not only required but, when performed properly, enhance the safety of classified data and diminish the risk of compromise.

FAA Has Not Made Long Overdue Updates to Its Classification Policy

FAA has not updated its 2006 policy on safeguarding classified national security information[11] to comply with the EO as required by ISOO. The EO required this policy be updated no later than December 25, 2010—almost 6 years ago. For example, the existing order does not contain provisions relating to complying with ancillary marking requirements of derivative classifier identity and declassification date. These are important because, for example, the absence of a date or an incorrect declassification date may result in the document being made public sooner than it should be, resulting in compromised classified information. We notified FAA about this issue in our 2013 report. At that time, FAA told us policy revisions had been affected by organizational changes and resources and agreed to correct the matter. However, during this audit, FAA informed us that the draft policy was still under review by management. These delays in updating a 10-year old policy are due to management's failure to use good judgement in prioritizing this critical task. Outdated policies increase the risk that documents will not be properly classified.

[11] FAA Order 1600.2E, Safeguarding Classified National Security Information (March 2006).

FAA's Performance Plans Do Not Address Classified Information

DOT's order on classified national security information, consistent with the EO, requires that OST and heads of OAs ensure that performance standards of all employees whose duties significantly involve the creation, handling, or management of classified information include management of classified information as a critical element to be evaluated in their ratings. While OST complied with this requirement, FAA did not. We obtained performance plan templates or performance plans for all sites in our sample. None contained the critical element. Without rating its employees on their handling of classified information, FAA management cannot use performance plans to motivate them to comply with classification requirements and decrease the deficiencies occurring in the program.

FAA's Self-Inspection Program Reports Are Incomplete or Contain Errors

FAA's self-inspection procedures do not fully comply with the EO's requirements, primarily because OST is not dedicating sufficient resources to oversee FAA's self-inspection program. The EO requires that heads of agencies that handle classified information designate a senior agency office responsible for establishing and maintaining an ongoing self-inspection program, which will include regular reviews of representative samples of the agency's original and derivative classification actions.

At FAA, the Servicing Security Elements (SSEs) are responsible for performing the self-inspections. SSE uses a checklist to perform these inspections; however, this checklist is mostly focused on safeguarding controls, such as the use of required forms. At the five locations in our sample, we did not find evidence that original or derivative classification actions were reviewed. We also noted some cases where the inspection revealed errors (e.g., overdue changes to safe combinations); yet the inspection report stated that "there were no findings noted during this inspection." Management was unaware of these errors prior to our review. Without comprehensive or accurate self-inspections, FAA cannot ensure that documents are properly classified, handled, and protected.

OST and FAA Classified Documents Are Not All Correctly Marked

Both OST and FAA had instances of document-marking errors in noncompliance with Federal regulations. We examined a random sample of 40 out of 168 classified documents at OST and 30 out of 708 classified documents at FAA. However, the errors we found pertained mostly to how the document was marked—not to missing markings (see table 2).

Table 2. Instances of Marking Errors at OST and FAA

Issue Description	Number of Instances at OST	Number of Instances at FAA	Totals
Overall document classification was at a higher level than content of document (overclassification).	3	3	**6**
Overall document classification was at a lower level than highest classification of portions of document (underclassification).	1	2	**3**
Document had incorrect declassification information.	1	7	**8**
Portions of documents did not follow portion- or caveat-marking format requirements.	22	25	**47**

Source: OIG analysis

This represents some improvement over our 2013 audit, which found that derivatively classified documents did not follow the ISOO control-marking requirements. At that time we estimated, based on our statistical sample, that about 72 percent (or 180 of the 248) of Confidential or Secret documents were marked incorrectly. This was largely due to problems with briefings and threat analyses that were missing required markings.

In our current audit, the most significant issues encountered were nine instances at OST and FAA where documents were marked but were either overclassified or underclassified. Overclassified documents increase the risk that information will not be available to a user who has a need to know but does not have the correct level of clearance. Underclassification increases the risk that sensitive information will be compromised.

- Based on the three overclassified and one underclassified document we found at OST, we estimate that 7.5 percent of all documents in the OST universe are overclassified,[12] and 2.5 percent of all documents in the OST universe are underclassified.[13]

- Based on the three overclassified and two underclassified documents we found at FAA, we estimate that 3.5 percent of documents in the FAA universe are

[12] Our 7.5 percent estimate has a 100-percent lower confidence limit of 1.8 percent and a 90-percent upper confidence limit of 13.6 percent.
[13] Our 2.5 percent estimate has a 100-percent lower confidence limit of 0.6 percent and a 90-percent upper confidence limit of 6.1 percent.

overclassified,[14] and 3.3 percent of documents in the FAA universe are underclassified.[15]

Other issues encountered were incorrect portion markings[16] or caveats[17]—with 22 of these errors in our OST sample of 40 classified documents and 25 in our FAA sample of 30 classified documents. Examples of these errors include a section of a document with a picture that was not marked or the use of an outdated caveat. Missing portion markings may require the user of a document to return to its source to identify the correct classification; outdated caveats may increase the risk that an inexperienced user may misunderstand the dissemination restrictions.

- Based on the 22 documents we found with these errors at OST, we estimate that 55 percent of all documents in the OST universe had portion- or caveat-marking issues.[18]

- Based on the 25 documents we found with these errors at FAA, we estimate that 79.6 percent of documents in the FAA universe had portion- or caveat-marking issues.[19]

We also found instances of documents that (1) cited multiple sources but not all sources were included and (2) did not identify the derivative classifier by name and title, contrary to ISOO requirements. OST and FAA officials were unaware of these matters prior to our review. Inadequately marked documents or portions of a document do not alert users to the sensitivity of the information and increase the risk that documents will be compromised.

Some OST and FAA Nondisclosure Forms Are Not on File

NARA[20] requires that individuals sign a classified information nondisclosure agreement, Standard Form 312 (SF-312), with the United States prior to accessing classified information. The SF-312, which is legally binding, spells out an individual's responsibilities in handling classified information. By signing, the employee agrees to comply with laws and regulations that prohibit unauthorized

[14] Our 3.5-percent estimate has an adjusted 100-percent lower confidence limit of 0.4 percent and a 90-percent upper confidence limit of 7.2 percent.
[15] Our 3.3-percent estimate has an adjusted 100-percent lower confidence limit of 0.3 percent and a 90-percent upper confidence limit of 8.3 percent.
[16] 32 CFR 2001.21(c) states: "Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which portions are unclassified by placing a parenthetical symbol immediately preceding the portion to which it applies."
[17] Caveats can be added to documents to control dissemination. For example, if distribution to non-US citizens is prohibited, regardless of clearance or access permissions, the caveat "NOFORN" should be added. "NOFORN" means "NOT RELEASABLE TO FOREIGN NATIONALS."
[18] Our 55-percent estimate has a 90-percent confidence limits ranging from 43.6 to 66.4 percent.
[19] Our 79.6-percent estimate has 90-percent confidence limits ranging from 63.1 to 96.1 percent.
[20] 32 CFR Parts 2001 and 2003 contain NARA/ISOO guidance, issued pursuant to Executive Order 13526, to agencies on original and derivative classification, downgrading, declassification, and safeguarding of classified national security information.

disclosure of classified information. NARA further requires that agencies retain the agreements for 50 years. However, we found several instances where these agreements were not on file, and management was unaware of the noncompliance. Of the sample items tested:

- For 50 of 125 FAA employees with active clearances, FAA did not have a signed SF-312 on file.

- For 6 of 36 DOT employees (excluding FAA) with active clearances, DOT did not have a signed SF-312 on file.

FAA management noted that 2 factors may have contributed to the absence of the 50 SF-312s. First, FAA recently discovered that an outdated form (SF-189) was being used instead of the SF-312 at some locations that still had supplies of the SF-189 on hand. Management further noted that this practice had been corrected. Second, FAA transitioned from hard files to fully electronic record keeping; this required the scanning of documents, some of which may have not been scanned properly and are now difficult to locate.

OST management stated that six employees arrived at DOT prior to 2010, and a different process was in place at that time. OST management further stated that as records are migrated to a new system that will be in place by the end of fiscal year 2016, a full review of the clearance holders' records will be performed, and any missing SF-312s will be immediately replaced.

Without a duly executed SF-312, an individual may not understand the importance of properly handling, or the consequences of mishandling, classified information. Consequently, there is an increased risk of compromise. The SF-312 form provides DOT with an important tool in pursuing administrative or legal action against an employee who compromises classified information.

FEW INSTANCES OF OVERCLASSIFICATION EXIST, BUT SOME PRACTICES MAKE IT POSSIBLE

Our review disclosed that instances of overclassification are estimated to be 7.5 percent at OST and about 3.5 percent at FAA (see table 2). While OST and FAA were unaware of these few instances, they do use ISOO guidance in preparing documents and, aside from these exceptions, conformed to this guidance. We also noted a practice that, while conforming to ISOO guidance, could result in cases of overclassification. Specifically, when DOT prepares a document for a briefing, it composes the document in a manner that is logical and helps the reader understand the issue in the proper context. To do this, a paragraph may contain information from various sources that have different

classification levels. DOT then marks the paragraph with the highest classification of any information in it. However, if this document is used as a source to develop another document, the preparer may assume all content in a paragraph is classified at the same level and may extract a portion of the paragraph that originally had a lesser classification, and mark the extracted information with the higher classification. As a result, information may become overclassified. While this is possible, we did not observe any instances at DOT where this occurred.

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 overclassification, and comply with Federal requirements. DOT has improved its practices and diminished risk, but some weaknesses persist in key areas like issuing policy and document marking. Until DOT takes additional actions to improve compliance with Federal requirements, it will be unable to ensure that national security information is adequately managed.

RECOMMENDATIONS

We recommend that DOT's Assistant Secretary for Administration:

1. Implement protocols or practices to identify DOT employees outside FAA who are missing nondisclosure forms and have each of these employees complete the agreement.

2. Implement protocols or practices to reinforce guidance on the marking of classified documents and to periodically assess compliance.

3. Dedicate additional resources to oversee FAA's self-inspection program.

We recommend that the Federal Aviation Administrator, in addition to issuing an updated policy as recommended in our prior report:

4. Implement protocols or practices to identify FAA employees who are missing nondisclosure forms and have each of these employees complete the agreement.

5. Implement protocols or practices to reinforce guidance on the marking of classified documents and to periodically assess compliance.

6. Identify all employees whose duties significantly involve the creation,

handling, or management of classified information, and update any performance plan that is missing a critical element on management of classified information.

7. Implement protocols or practices to enhance the quality of self-inspection reports and to periodically assess compliance.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided OST with our draft report on September 29, 2016, and received its response on October 31, 2016, which is included as an appendix to this report. OST concurred with seven recommendations as written.

OST requested that we close recommendations 1 and 2. However, the documentation received from OST did not fully meet the intent of our recommendations. For recommendation 1, the information did not include the protocol or practices to identify the missing nondisclosure forms. For recommendation 2, the information did not include protocol or practices to reinforce guidance on marking of classified documents, including periodically assessing compliance. Until we receive the needed information, we consider both recommendations to be open and unresolved.

ACTIONS REQUIRED

OST and FAA provided appropriate planned actions and timeframes for recommendations 3, 4, 5, 6, and 7, and we consider them resolved but open pending completion of the planned actions. We consider recommendations 1 and 2 open and unresolved and request that OST provide us with the information requested above as well as target completion dates within 30 days of the date of this report in accordance with DOT Order 8000.1C.

We appreciate the courtesies and cooperation of DOT and FAA representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407 or Lissette Mercado, Information Technology Audits Advisor, at (202) 366-1911.

#

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

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted our work from July 2015 through September 2016. We conducted our audit work 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.

Our objectives were to (1) assess whether DOT has implemented policies and procedures to classify information effectively that comply with Federal policy and regulations and (2) identify any practices that may lead to persistent misclassification of information.

To conduct this performance audit, we did the following:

- Reviewed Federal policy, rules and regulations,
- Reviewed agency policy, procedures and practices,
- Interviewed officials responsible for managing DOT's classified national security information program,
- Interviewed a sample of employees with security clearances using questions provided by the ISOO,
- We interviewed 39 DOT employees whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings at the Crisis Management Center, OST Intelligence Division, and MARAD's Command Center.
- Conducted site visits,
- Reviewed a sample of classified documents, and
- Coordinated with the ISOO.

To ensure accuracy and completeness of the employee and classified documentation listings we received from DOT and FAA, we reviewed documentation, conducted interviews, sampled employees and records, and validated the Department's records in the DOT and FAA training data repositories.

Based on our review we deemed the Department's listings sufficiently reliable for

the purposes of our audit.

We verified that OST has a universe of 168 classified documents from which we selected a simple random sample of 49. Due to resource constraints, we reviewed a total of 40 classified documents, which allowed us to estimate the noncompliance rate with a precision of no more than +/-11.4 percent at the 90-percent confidence level. We also obtained a universe of 708 classified documents from FAA which we stratified by type into 8 strata and selected a proportional simple random sample from each stratum for a total sample size of 62. Due to resource constraints, we reviewed a total of 30 classified documents, which allowed us to estimate a noncompliance rate with a maximum precision of +/-16.5 percent at the 90-percent confidence level.

We obtained a listing with 10,309 FAA employees with active clearances from an FAA official who retrieved it from the Investigative Tracking System. We selected a 2-stage sample as follows: We aggregated the number of employees by city, and included all cities that had 10 or more employees in our Stage 1 universe. Our Stage 1 universe had 55 cities with 9,801 employees. From that Stage 1 universe we selected a sample of 5 out of 55 FAA cities with probability proportional to size with replacement where size was the number of employees at each city. Stage 2 was a simple random sample of 25 employees from each city selected in Stage 1 for a total of 125 employees. We did not project the results of this sample.

EXHIBIT B. STATUS OF PRIOR RECOMMENDATIONS

Recommendation	Status
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).	Closed
Seek additional resources to complete comprehensive self-inspections, and to prepare accurate reports to NARA's Information Security Oversight Office.	Closed
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.	Closed
Establish a procedure and communicate to the OAs clear definitions and requirements for ensuring that annual reporting to the NARA's Information Security Oversight Office is accurate and complete.	Closed
Update FAA's policy to conform to the requirements of EO 13526.	OPEN

EXHIBIT C. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Abdil Salah	Program Director
Lissette Mercado	Information Technology Audits Advisor
James Mullen	IT Specialist
Thomas Summers	Auditor
Zachary Lewkowicz	IT Specialist
Petra Swartzlander	Senior Statistician
Makesi Ormond	Statistician
William Savage	IT Specialist
Andrea Nossaman	Senior Writer-Editor
Jane Lusaka	Writer-Editor
Amy Berks	Senior Counsel

Memorandum

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

Subject: INFORMATION: Management Response to the Office of Inspector General (OIG) Draft Report – *Improvements Increase DOT's Compliance With The Reducing Over-Classification Act*

Date: **OCT 31 2016**

From: Jeff Marootian
Assistant Secretary for Administration

To: Louis C. King
Assistant Inspector General for
Financial and Information Technology Audits

Information security is a priority for the U.S. Department of Transportation (DOT). We are committed to ensuring that national security information is classified, safeguarded, and declassified in accordance with all Federal requirements. As the OIG noted in its draft report, DOT has improved its classification practices and diminished risks since OIG's prior review in 2013. Further, the National Archives and Records Administration Information Security Oversight Office (ISOO) recently conducted an audit of DOT's classification marking practices. ISOO found no errors in our marking practices and cited our "exemplary" oversight process.

We have several efforts under way or completed to further enhance the Department's management of classified national security information. For example, DOT:

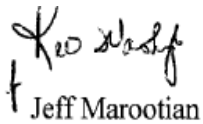
- implemented procedures to ensure all employee classified nondisclosure agreements are correctly filed and retained;
- instituted a new oversight process for the marking of classified documents to include both peer and manager review that is producing error-free intelligence products; and
- Identified Federal Aviation Administration (FAA) positions with significant duties in the management, designation, and marking of classified information, and we are updating performance plans for these positions.

Based on our review of the draft report, we concur with all seven recommendations as written. We have provided OIG with documentation that shows we have completed actions to implement recommendations 1 and 2, and we request closure. We plan to complete actions to implement the remaining recommendations as follows: recommendation 3 by September 30, 2019;

recommendation 4 by April 20, 2017; recommendations 5 and 7 by January 31, 2017; and recommendation 6 by September 30, 2017.

We appreciate the opportunity to review the OIG draft report. Please contact Joan Harris, Associate Director for Security Policy, at 202-366-1827 with any questions.

Sincerely,



Jeff Marootian
Assistant Secretary for Administration

Appendix. Agency Comments