OFFICE OF INSPECTOR GENERAL

DHS Has Not Trained Classified Network Users on the Classification Management Tool

Homeland Security

September 26, 2016

OIG-16-141

DHS OIG Highlights

DHS Has Not Trained Classified Network Users on the Classification Management Tool

September 26, 2016

Why We Did This Inspection

The *Reducing Over- Classification Act* requires Federal Government Inspectors General of departments that make original classification determinations to conduct no less than two evaluations of their agencies' classification policies, procedures, rules, and regulations. The Department of Homeland Security (DHS) implemented the two recommendations from our first evaluation. In this second evaluation, we assessed DHS' progress in its classification management program after implementing the recommendations.

What We Recommend

We recommend that the DHS Office of the Chief Security Officer train new classified network users on the CMT and offer refresher training to current users.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

In 2014, DHS deployed a new classification management tool (CMT) to help users properly mark classified documents and emails. However, the Department has not trained employees on using the CMT. As a result, employees reported they had difficulty using the tool when marking and sending classified emails. We also reviewed 269 classified documents and identified 48 classification marking errors, which resulted in an error rate similar to the rate we identified during our 2013 document review. Training, as well as using the CMT when creating these documents, would help employees identify and correct many of these errors. Without such training, DHS will not realize the full potential of the CMT.

DHS Response

DHS officials concurred with the recommendation. DHS has proposed steps to improve CMT training for classified network users. We consider the recommendation open and resolved.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 26, 2016

MEMORANDUM FOR: The Honorable Russell C. Deyo
Under Secretary for Management
Department of Homeland Security

FROM: John Roth
Inspector General

SUBJECT: *DHS Has Not Trained Classified Network Users on the Classification Management Tool*

For your action is our final report, *DHS Has Not Trained Classified Network Users on the Classification Management Tool.* We incorporated the formal comments provided by your office.

The report contains one recommendation aimed at improving classification management tool training for classified network users. Your office concurred with the recommendation. Based on information provided in your response to the draft report, we consider this recommendation open and resolved. Once your office has fully implemented the recommendation, please submit a formal closeout letter to us within 30 days so that we may close the recommendation. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions.

Please send your response or closure request to OIGInspectionsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to 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 Anne L. Richards, Assistant Inspector General for Inspections and Evaluations, at (202) 254-4100.

Background

On December 29, 2009, the President signed Executive Order 13526, *Classified National Security Information*, prescribing a uniform system for classifying, safeguarding, and declassifying national security information. The three categories of U.S. Government classification, and correlating expected damage if released without authorization, are:

- Top Secret – unauthorized disclosure of this information could reasonably be expected to cause *exceptionally grave damage* to national security;
- Secret – unauthorized disclosure of this information could reasonably be expected to cause *serious damage* to national security; and
- Confidential – unauthorized disclosure of this information could reasonably be expected to cause *damage* to national security.

On October 7, 2010, Congress passed Public Law 111-258, *Reducing Over-Classification Act,* requiring the Secretary of DHS to develop a strategy to prevent over-classification and promote information sharing. The act also requires Federal Government Inspectors General of departments that make original classification determinations to conduct no less than two evaluations of their agencies to:

- assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered; and
- identify policies, procedures, rules, regulations, or management practices that may contribute to persistent mis-classifying of information.

In August 2013, the DHS Office of Inspector General (OIG) issued its first evaluation, *Reducing Over-classification of DHS' National Security Information* (OIG-13-106). We concluded that DHS had adopted and successfully implemented all policies and procedures required by applicable Federal regulations, Intelligence Community directives, and the DHS Office of Chief Security Officer (OCSO). Also, in reviewing 372 documents classified by DHS components, we identified 59 errors related to classification marking. To further strengthen its classification program, we recommended that DHS:

- fully deploy a new classification management tool (CMT) to all components and offices when it completed testing the tool; and
- create and implement a standard method for components to collect and report information for the Standard Form 311, *Agency Security Classification Management Program Data* (SF-311).[1]

To address the first recommendation, in April 2014, DHS deployed a new CMT. The Intelligence Community uses the CMT as a standard for applying classification and control markings when creating documents electronically and when emailing classified documents. To assist in creating classified documents, the CMT is integrated into Microsoft Word, PowerPoint, and Excel; to email classified documents, the CMT is integrated into Outlook.

To address the second recommendation, in September 2014, DHS changed its method for collecting and reporting classification management data on the SF-311. DHS uses the SF-311 to collect and record classification decisions and provide classification management data annually to the Information Security Oversight Office (ISOO) at the National Archives and Records Administration. ISOO compiles the information from the agencies in a report for the President.

The DHS OCSO proposed standard procedures to count the Department's classification decisions. The new procedures decreased the reporting period from 12 months to 3 months (April to July) to encourage users[2] to focus their attention on tracking classification decisions during this period. To standardize and simplify the collection process, DHS uses the 311A form, which provides specific accounting instructions for recording individual classification decisions. DHS continues to follow these standard procedures to track classification decisions.

Because DHS took these actions, we closed both recommendations from our August 2013 evaluation. In this second evaluation, we assessed DHS' progress in its classification management program after implementing the recommendations.

[1] Per 32 CFR 2001.80(d)(1), the SF-311 is a data collection form completed only by those executive branch agencies that create and/or handle classified national security information.
[2] Users are individuals with access to classified networks.

Results of Inspection

In 2014, DHS deployed a new CMT to help users properly mark classified documents and emails. However, the Department has not trained employees on using the CMT. As a result, some employees reported they had difficulty using the tool when marking and sending classified emails. We also reviewed 269 classified documents and identified 48 classification marking errors, which resulted in an error rate similar to the rate we identified during our 2013 document review. Training, as well as using the CMT when creating these documents, would help employees identify and correct many of these errors. Without such training, DHS will not realize the full potential of the CMT.

DHS Did Not Adequately Train Employees on Using the CMT

About 30 days before installing the CMT in February 2014, the Department emailed users an internet link to CMT training materials. Since that time, however, DHS has not provided further training to any users, including anyone who began using the CMT after its February 2014 deployment. Of the users we interviewed, only a few said they were aware of training materials for the CMT. As a result, when attempting to mark and send an email with classified information, users had difficulty navigating through the CMT.

Before implementing the CMT, DHS created a working group to determine the best way to conduct training for CMT users. The working group discussed customized training, but could not reach consensus on whether the Department should conduct training in a classified or unclassified environment and whether the training should be computer based or led by an instructor. The working group decided an internet link to the CMT user manual and training videos from the developer was sufficient for CMT users.

In response to the first recommendation from our August 2013 evaluation, DHS wrote that "concurrent to full deployment and for a period of time thereafter" the OCSO would conduct "initial individualized training essential to the successful deployment and use of the tool." However, this did not occur. DHS simply provided access to training materials once before deployment.

On January 7, 2014, about 30 days before the CMT launched on DHS' classified local area network (C-LAN),[3] the DHS Enterprise Networked Services Support team emailed C-LAN users informing them about the CMT deployment. The email also contained a link directing users to a non-DHS website to access the CMT user guide and a series of training videos. The Department has not provided this training link to anyone since deploying the CMT.

[3] The C-LAN is DHS' Top Secret network.

Of the 102 users we interviewed, only 9 said they "received" CMT training. Other users said they did not receive training, were unaware of the email link, or obtained help from security managers or more experienced users.

Without training, some users lacked familiarity with the CMT, which decreased the efficiency of email dissemination. For example, when users initially tried to send an email, different tabs appeared without warnings or instructions. Several interviewees said that new C-LAN users need training before accessing the CMT. According to some users, the CMT is not "user-friendly" and can be overwhelming for individuals with little experience.

The CMT Helps Users Identify and Correct Classification Marking Errors

Before deploying the CMT in 2014, DHS did not have a department-wide, standard classification tool on its classified networks. The components used various tools that did not comply with Federal and Intelligence Community classification marking guidelines. These tools prevented users from marking classified information properly. Additionally, users could incorrectly mark email and send information without verifying the classification markings.

Of the 102 users we interviewed, 59 said the current CMT is more effective than previous classification tools in identifying and helping to correct classification errors. The CMT helps users apply correctly formatted classification markings to emails and electronic documents. When users select a classification level (Top Secret, Secret, or Confidential), the CMT generates a series of steps to apply the appropriate portion markings, classification banners (header and footer), and a classification authority block.[4] The CMT then ensures the classification level in the banner is consistent with the highest classification level in the portion markings. For example, if a portion of a document is marked Top Secret, the overall classification of the email cannot be Secret or Confidential. The CMT would warn and prevent the user from sending the email. The CMT cannot stop a user from over- or under-classifying an email if all classification markings are consistent, but it has fail-safes to prevent most errors.

Components' Classified Documents Contained Some Classification Errors

In our 2013 evaluation, we reviewed 372 classified documents from DHS components and identified 59 classification marking errors. To identify trends in classification errors, in this evaluation, we reviewed 269 classified documents from 14 DHS components:

[4] The classification authority block contains the source information, declassification date, and the classifier.

- U.S. Customs and Border Protection
- Domestic Nuclear Detection Office
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Office of Intelligence and Analysis
- U.S. Immigration and Customs Enforcement
- National Programs and Protection Directorate
- Office of Operations Coordination
- Office of Policy
- Science and Technology Directorate
- Transportation Security Administration
- U.S. Citizenship and Immigration Services
- U.S. Coast Guard
- U.S. Secret Service

In the 269 documents, we identified 48 classification marking errors, including missing classification blocks, incorrect portion markings, and not listing multiple sources of information. Appendix B contains details on the types of documents we reviewed and the errors we identified.

Of the 48 errors, 25 were missing classification blocks in email attachments.[5] This type of error does not reflect a problem with the CMT. The CMT will ensure the user properly applies classification markings, including the classification block. Therefore, users can avoid these errors if they use the CMT when creating email attachments. In these cases, users may have chosen not to use or did not think they had to use the CMT when creating an attachment. Other users may have been unaware of the CMT's capability, which training should correct. Without such training, DHS will not realize the full potential of the CMT and may continue to make errors marking classified documents.

Recommendation

We recommend that the DHS Chief Security Officer:

Recommendation: Train new classified network users on the classification management tool and offer refresher training to current users.

[5] Attachments may include Microsoft Word documents, PowerPoint presentations, and Excel spreadsheets.

Management Comments and OIG Analysis

The Department concurred with our recommendation. A summary of DHS' response and our analysis follows. We have included a copy of the management comments in their entirety in appendix A. DHS also provided technical comments, which we incorporated as appropriate.

DHS Response: DHS agrees that the CMT has the potential to reduce derivative classification errors. OCSO will continue to provide CMT training in its derivative classification training courses. In addition, OCSO will coordinate with the Office of Intelligence and Analysis (I&A), which owns the Top Secret/Sensitive Compartmented Information (TS/SCI) network, to ensure a communication link to the CMT manual is sent out via email to all network users. I&A will also coordinate with the Homeland Secure Data Network (HSDN) Program Management Office to send out the link to the CMT manual for HSDN users. Lastly, OCSO will incorporate the CMT manual link into required annual Information Technology security training for those with TS/SCI clearances. The expected completion date is October 31, 2016.

OIG Analysis: We acknowledge that DHS' required biennial derivative classification training references CMT training; however, the information presented on the CMT should be more robust. Derivative classification training is a classified network user's first exposure to derivative classifications and use of classified systems. Training should explain all available tools to help users properly mark classified information. DHS' plans to provide the CMT training link via email to B-LAN and C-LAN users will notify new and current users of the training materials available for the CMT. In addition, DHS' plan to incorporate the CMT manual link within other required security training will help ensure users receive access to CMT training materials on an annual basis.

We consider DHS' proposed actions responsive to the intent of the recommendation, which is open and resolved. We will close the recommendation pending completion of the proposed corrective actions and submission of adequate supporting documentation.

Objective, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

The objectives of the inspection were to assess whether DHS adopted, followed, and effectively administered applicable classification policies, procedures, rules, and regulations within the Department; and if classification issues exist, identify policies, procedures, rules, regulations, or management practices that may contribute to over-classifying information within DHS.

To achieve our objectives, we examined executive orders, public laws, and policies governing DHS' handling of national security information. We also reviewed:

- Classified documents from components
- Security classification guides and procedures
- CMT training manual
- SF-311 data

We interviewed officials from DHS' OCSO; U.S. Customs and Border Protection; Domestic Nuclear Detection Office; Office of the Executive Secretariat; Federal Emergency Management Agency; Federal Law Enforcement Training Center; Office of Intelligence and Analysis; U.S. Immigration and Customs Enforcement; and National Programs and Protection Directorate. In addition, we interviewed staff from DHS' Office of Health Affairs, Operations Coordination; Office of Policy; Science and Technology Directorate; Transportation Security Administration; U.S. Citizenship and Immigration Services; U.S. Coast Guard; U.S. Secret Service; and National Archives and Records Administration.

We conducted this review between January and June 2016 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.

The Office of Inspections and Evaluations' major contributors to this report are William McCarron, Chief Inspector; LaDana Crowell, Senior Inspector; Anthony Crawford, Intelligence Officer; Adam Brown, Senior Inspector; Kelly Herberger, Communications Analyst; and Renita Hunter, Independent Reference Review.

Appendix A
DHS Comments to the Draft Report

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

Homeland Security

September 8, 2016

MEMORANDUM FOR: John Roth
Inspector General

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

SUBJECT: Management's Response to OIG Draft Report: "DHS Has Not Trained Classified Network Users on the Classification Management Tool" (Project No. 16-013-ISP-DHS)

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

The Department is pleased to note the OIG's positive recognition of our adoption and successful implementation of policies and procedures required by Public Law 111-258, "Reducing Over-Classification Act" and other regulations and directives to help prevent over-classification and promote information sharing. DHS will continue protecting information critical to our Nation's security and demonstrating our commitment to open Government through the accurate and accountable application of classification standards.

It is important to clarify, however, that contrary to the impression OIG's report may leave with some readers, Classification Management Tool (CMT) training is not absent from required DHS security classification training. For example, as part of the Office of the Chief Security Officer's (OCSO) "Understanding Derivative Classification and Marking" training course[1], instructors do reference the CMT, describing how declassification exemptions can be properly entered, how declassification exemptions that are no longer valid are entered, and how the CMT automatically runs as part of Microsoft Outlook. CMT instruction is also incorporated into other OCSO courses, such as the "Train-the-Trainer for Understanding Derivative Classification and Marking" course, in response to classroom feedback on areas where participants have encountered issues with the tool, as appropriate.

[1] This biennial course is mandated for all DHS employees, civilian, military, detailees, or contractor personnel performing duties that require a fundamental understanding of how to properly mark classified information or who have a classified network account.

In addition, readers of the OIG's report should know that in February 2016, the National Archives and Records Administration's Information Security Oversight Office (ISOO)[2] conducted a review of DHS classification practices, including training, and in its final report stated:

> "The DHS has an excellent security and training program. It provides the required forms of security education and training, including initial training, annual refresher training, termination briefings, specialized training, derivative classification training, and training for original classification authorities."
>
> "The DHS also provides excellent training on the creation and use of security classification guides and on risk management principles. In addition, the DHS provides outstanding training for security specialists. Personnel we interviewed spoke highly of the training they received and commented favorably on the face-to-face training that included practical exercises on the marking of documents."

The draft report contained one recommendation with which the Department concurs. Attached find our detailed response to this recommendation.

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

Attachment

[2] The ISOO is responsible to the President for policy and oversight of the Government-wide security classification system. The Operations Staff evaluates the effectiveness of the security classification programs established by Government and industry to protect information vital to our national security interests.

Attachment: DHS Management Response to Recommendations Contained in 16-013-ISP-DHS

The OIG recommended that the DHS Office of the Chief Security Officer:

Recommendation: Train new classified network users on the CMT and offer refresher training to current users.

Response: Concur. DHS agrees that the CMT has the potential to reduce derivative classification errors. OCSO will continue to provide CMT training in its derivative classification training courses. In addition, OCSO will coordinate with the Office of Intelligence and Analysis (I&A), which owns the Top Secret/Sensitive Compartmented Information (TS/SCI) network, to ensure a communication link to the CMT manual is sent out via email to all network users. I&A will also coordinate with the Homeland Secure Data Network Program Management Office to send out the link to the CMT manual for this system's users. Lastly, OCSO will incorporate the CMT manual link into required annual Information Technology security training for those with TS/SCI clearances. Estimated Completion Date: October 31, 2016.

Appendix B
Classified Document Review Results

LEVEL OF CLASSIFICATION	
Top Secret/SCI	42
Top Secret	33
Secret/SCI	6
Secret	179
Confidential	9
TOTAL	**269**

TYPE OF DOCUMENT	
Cable/Message	1
Memo/Letter	26
Electronic Media/Email/Slide Presentations	67
Reports	151
Other (Intelligence Assessments and Notes, Briefings, Issue Papers, Talking Points)	24
TOTAL	**269**

ERRORS	
Duration of Classification	2
Unknown Basis for Classification/"Derived From" Line	3
Portion Marking	5
Multiple Sources (not listed)	10
Marking	3
Other (no classification block)	25
TOTAL	**48**

Appendix C
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs 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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

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