Audit Report

OIG-16-059

GENERAL MANAGEMENT: Treasury Has Policies and Procedures to Safeguard Classified Information But They Are Not Effectively Implemented

September 29, 2016

Office of Inspector General

Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

Contents

Abbreviations

E.O.	Executive Order
ISOO	Information Security Oversight Office
JAMES	Joint Audit Management Enterprise System
OCA	original classification authority
OSP	Office of Security Programs
SF	standard form
TD P	Treasury Directive Publication
TFI	Office of Terrorism and Financial Intelligence
TLMS	Treasury Learning Management System

September 29, 2016

S. Leslie Ireland
Assistant Secretary for Intelligence and Analysis

This report provides the results of our second evaluation of the Department of the Treasury's (Treasury) classification program, pursuant to Public Law 111-258, *Reducing Over-Classification Act* (the Act). The Act requires the Inspectors General of each department or agency of the United States with an officer or employee who is authorized to make original classification[1] decisions to evaluate the agency's classification program and identify practices that may contribute to the persistent misclassification[2] of material. The Act requires that we conduct two evaluations. We issued our first evaluation report in September 2013.[3]

In accordance with the Act, the evaluation objectives were to (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within Treasury; and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to the persistent misclassification of material within Treasury.

As required by the Act, we coordinated with other Inspectors General who were required to conduct the same evaluation of their agencies. To accomplish our objectives, we used an evaluation

[1] Original classification is the determination by an authorized official that information within specifically designated categories requires protection against unauthorized disclosure in the interest of national security. Individuals authorized to make this original determination have original classification authority (OCA) and are authorized in writing, either by the President, the Vice President, agency heads, or other officials designated by the President. Treasury has 13 officials with OCA.

[2] Misclassification is the act of incorrectly classifying, either over- or under-classifying, information.

[3] *Treasury Has Policies and Procedures to Safeguard Classified Information But Implementation Needs to Be Improved,* (OIG-13-055; issued Sep. 27, 2013).

guide that was prepared by a working group of participating Offices of Inspector General on behalf of the Council of the Inspectors General on Integrity and Efficiency.[4] We performed our fieldwork from November 2015 through June 2016. Appendix 1 contains a more detailed description of our evaluation objectives, scope, and methodology.

In brief, Treasury has put policies and procedures in place to safeguard classified materials, but continues to have difficulty ensuring that these policies and procedures are consistently followed. Our findings in this evaluation are similar to those identified in our 2013 report. We noted continuing concerns with (1) marking classification decisions;[5] (2) completing the Standard Form (SF) 311, *Agency Security Classification Management Program Data;*[6] and (3) complying with self-inspection[7] requirements. In addition, we identified a new area of weakness - inadequate maintenance of security training documentation. We are making seven recommendations to improve the classification management process.

In a written response, the Office of Intelligence and Analysis[8] concurs with our recommendations and the Assistant Secretary

[4] Department of Defense Office of Inspector General, *A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, Reducing Over-Classification Act* (Jan. 22, 2013).

[5] Marking is the act of properly labeling sections of classified documents, whether paper copies or electronic, to indicate (1) the overall level of classification, (2) the paragraph/portion classification, (3) the name and position or personal identifier of the classifier, (4) the reason or source of the classification, and (5) the date or event for declassification.

[6] The SF 311 is used to collect data from Executive branch agencies that create and/or handle classified national security information. Information to be reported includes the number of (1) individuals designated with OCA, (2) original and derivative classification decisions, (3) mandatory declassification review requests and appeals, (4) pages of decisions declassified, (5) internal oversight activities including self-inspections conducted, and (6) classification guides created and used. Classification decisions refer to any recorded information, including documents and e-mails.

[7] Self-inspections are internal reviews and evaluations conducted by agency management for activities related to classified information. For the Treasury classification management program, the Office of Security Programs conducts self-inspections of Treasury's Departmental Offices; however, bureaus are responsible for conducting self-inspections of their classification management programs.

[8] Treasury's Office of Intelligence and Analysis was established within Treasury by Public Law 108-177, *Intelligence Authorization Act for Fiscal Year 2004* (Dec. 13, 2003). The office is responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of Treasury.

provided corrective actions taken and planned to implement our recommendations. The management response is summarized in the Findings sections of the report and the text of the response is included in its entirety at appendix 2. We believe the corrective actions, taken and planned, are responsive to our recommendations.

Background

In 2009, the President signed Executive Order (E.O.) 13526,[9] *Classified National Security Information,* which updated classification principles, policies, and procedures and prescribed a uniform system for classifying, safeguarding, and declassifying[10] national security information. In addition, 32 C.F.R. § 2001, *Classified National Security Information,*[11] assists in implementing E.O. 13526 and sets forth related guidance.

E.O. 13526 requires heads of agencies that have employees with original classification authority (OCA) or who handle classified information to designate a senior agency official who is responsible for the classification management process. Within Treasury, the designated senior agency official is the Deputy Assistant Secretary for Security in the Office of Intelligence and Analysis.[12] The Deputy Assistant Secretary has oversight of the Office of Security Programs (OSP) and the Office of Special Security Programs.

The *Reducing Over-Classification Act*, which became law in 2010, was intended to address classification and information sharing issues highlighted by the *9/11 Commission Report.*[13] The Act

[9] E.O. 13526 rescinded E.O. 12958.

[10] Declassification is the authorized change in the status of information from classified to unclassified based on the duration of the national security sensitivity of the information.

[11] Effective June 25, 2010.

[12] Treasury's Office of Intelligence and Analysis was established within Treasury by Public Law 108-177, *Intelligence Authorization Act for Fiscal Year 2004* (Dec. 13, 2003). The office, which is headed by the Assistant Secretary for Intelligence and Analysis, is responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of Treasury.

[13] The *9/11 Commission Report* concluded that over-classification and inadequate information sharing contributed to the government's failure to prevent the attacks of 9/11. The report also stated that security requirements nurtured over-classification and excessive compartmentalization of information among agencies.

establishes procedures to promote information sharing with state, local, tribal, and private sector entities; and promote accurate classification of information by federal employees.

Evaluation Results

OSP is responsible for establishing Treasury policies and procedures for classification management based on E.O. 13526 and other federal sources. The *Treasury Security Manual* defines and implements Treasury's classification management policies.[14] OSP is also responsible for (1) developing security training programs, (2) monitoring Departmental Offices' and bureaus' compliance with federal and Treasury requirements for classified information, (3) reporting on Treasury's information security programs to the Information Security Oversight Office (ISOO),[15] and (4) representing Treasury interests on interagency forums.

While we determined that Treasury has put policies and procedures in place to safeguard classified materials, we found that Treasury has difficulty ensuring that these policies and procedures are consistently followed.

Finding 1 Classification Decisions Are Missing Required Markings

According to 32 C.F.R. § 2001.20, classification markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.[16] In addition, derivative classification decisions, including emails, shall bear (1) a classification authority block;[17] (2) an overall marking; (3) portion markings; (4) dissemination controls and handling markings; (5) the date of origin; and (6) a subject line.[18] The *Treasury Security*

[14] Treasury Directive Publication (TD P) 15-71, *General Information, Treasury and Bureau Responsibilities* (June 17, 2011).

[15] ISOO is an office within the National Archives and Records Administration responsible for policy and oversight of the Government-wide security classification system.

[16] 32 C.F.R. § 2001.20, *Identification and Markings, General* (June 28, 2010).

[17] The classification authority block consists of (1) a "Classified by" line to identify who prepared the document, (2) a "Derived from" line to explain the reason for the classification, and (3) a "Declassify on" line to indicate the length of the classification.

[18] 32 C.F.R. § 2001.22, *Identification and Markings, Derivative classification* (June 28, 2010).

Manual requires original and derivative classifiers to properly mark classified information they generate and avoid over-classifying information. To avoid errors in classifying email responses, the manual requires email chains with classified information to include required markings assigned to particular information to remain constant and email responses that do not contain classified information to be contained in a new unclassified email.[19] An example of a properly classified email is included as exhibit 1 on the next page. Even though the example is for an email, the same classification markings are required for non-emails.

Our review of a non-statistical sample of 108 derivative classification decisions (71 emails and 37 non-emails), selected from the population of 147,785 derivative classification decisions reported in Treasury's fiscal year 2015 SF 311, disclosed that 97 of the decisions (90 percent of the sample) contained one or more errors.[20] These errors related to the classification authority block, portion markings, dissemination control markings, and email responses.

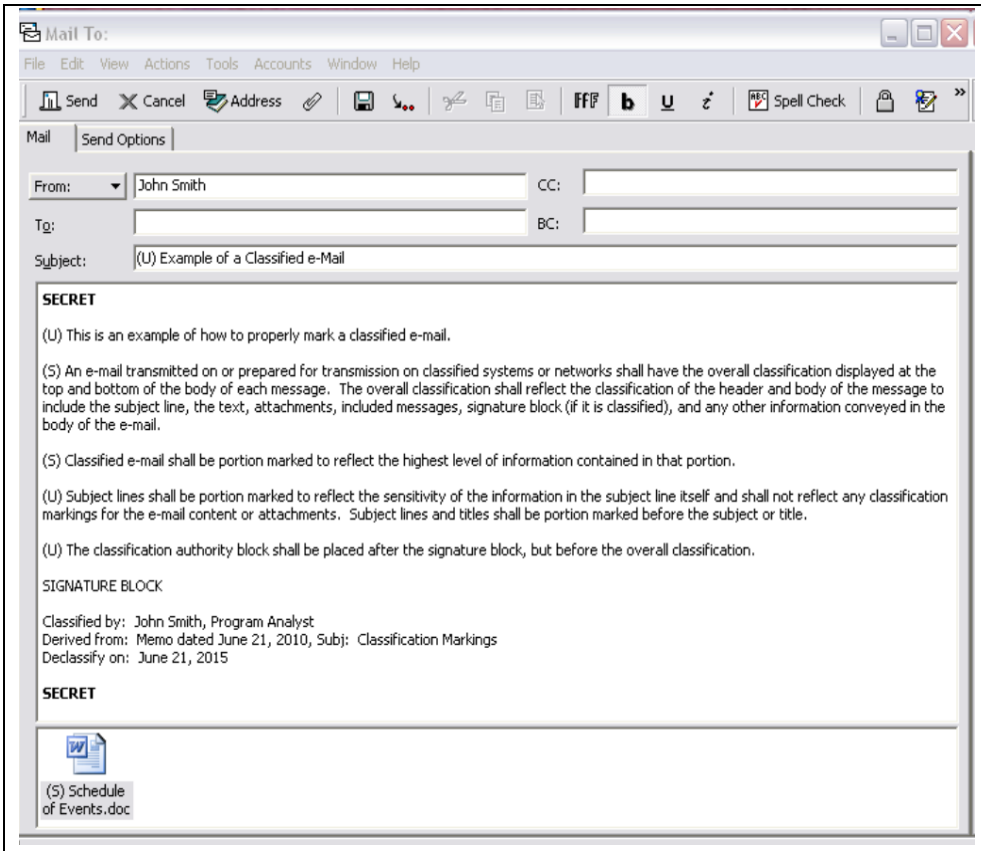
Specific errors we found on the decisions we reviewed in our sample include:

- Seventy-nine (79) of 108, or 73 percent, derivative classification decisions had incorrect portion markings on the subject line, paragraphs, or attachments. Sixty-six (66) of the 79 derivative classification decisions were emails and most of them did not contain any of the required portion markings, for example, the "(U)", "(S)", or similar marking.

[19] TD P 15-71, Chapter III, Section 5, *Original and Derivative Classification* (June 20, 2014).

[20] The sample was selected to obtain a cross-section of Treasury offices and bureaus and the types of decisions reported on Treasury's consolidated SF 311. Such decisions included emails, reports, official correspondence, memoranda, and presentations. The sample was not selected for the purpose of projecting to the population, and as such, we do not make a projection. See the description of our objectives, scope, and methodology in appendix 1 for more details of our sampling approach.

Exhibit 1. Example of a Properly Marked Derivative Classification Email Decision



Source: ISOO's *Marking Classified National Security Information* (January 2014)

Auditor's Notes – Whether as emails or non-emails, all classification decisions require the following items:

(1) The "(U)" and "(S)" are examples of portion or paragraph markings used. The "(U)" means unclassified and the "(S)" means secret.

(2) The word "**SECRET**" at the top and bottom of the page is the overall marking, or the banner. The banner and portion markings may also include a dissemination control or handling marking which further restricts access, for example, "NOFORN" means "no foreign" access.

(3) The text after the signature block is the classification authority block and it includes: (1) the classifier and his or her position in the "Classified by" line; (2) the source of the classified information in the "Derived from" line; and (3) the date that the classification period expires in the "Declassify on" line.

- Fifty-four (54) of 108, or 50 percent, derivative classification decisions contained errors in the classification authority block. Specifically, the decisions had (i) a missing classification authority block; (ii) the wrong classifier name or missing classifier position on the "Classified by" line; (iii) an outdated phrase, "Derived by" instead of "Classified by"; (iv) outdated classification guide in the "Derived from" line; and/or (v) a wrong date on the "Declassify on" line.

- Thirteen (13) of 108, or 12 percent, derivative classification decisions had missing or incorrect dissemination control markings. An example of dissemination control is the marking "NOFORN" in the banner or "(NF)" in the portion marking. In this case, the dissemination control marking is used to restrict the release of information in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator.

- Eighteen (18) of 71 emails, or 25 percent, derivative classification decisions had weaknesses specific to emails, including responses in an email chain for which the sender classified the information in the response at a lower level than the original email, and responses for which the sender continued the email chain even though the response was unclassified.

As stated in E.O. 13526, protecting information critical to our Nation's security and demonstrating our commitment to open government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities. The high rate of mismarked derivative classification decisions subjects Treasury to increased risks - both that classified information will not be adequately protected and that information that could be shared may not be disseminated to partnering agencies.

During our interviews with employees, we found that some may not understand the importance of properly marking emails. Others told us that they understand the requirement to properly mark emails but that they are too busy and it is unrealistic to portion mark all emails.

Recommendation

We recommend that the Assistant Secretary for Intelligence and Analysis direct the Deputy Assistant Secretary for Security to emphasize to derivative classifiers the importance of properly marking classification decisions, including adding a note in classified emails to remind employees to properly portion mark emails before sending.

Management Comments

OSP is revising the training program to include reminding authorized employees of the obligation to properly mark and safeguard classified information. OSP is coordinating with the Office of Special Security Programs to develop a security training campaign to include training on derivative classification decisions and portion markings. The revised training will enhance the current training provided to employees when they initially receive their security clearance for access to classified information and the annual security refresher training. OSP is also developing additional comprehensive and tailored training for Departmental Offices and bureaus. OSP will coordinate with Treasury Learning Management System (TLMS)[21] officials to ensure that training is included in the Security Program section of TLMS and accessible to bureau personnel.

While training materials are being revised, OSP has put in place two actions to increase awareness of the importance of properly marking classification decisions. OSP placed updated copies of the ISOO *Marking Classified National Security Information* guide in all of the Sensitive Compartmented Information Facilities, commonly referred as SCIF, for employee reference purposes. OSP has also launched a review of marking policy in the *Treasury Security*

[21] TLMS helps ensure all training is compliant with federal regulations, and provides manager reports in one convenient interface and technology package in accordance with the Office of Personnel Management mandate that requires all federal agencies to use a learning management system to account fully for federal professional development activity.

Manual to determine whether to allow for the same flexibility authorized by the ISOO in its implementing regulation.[22]

OIG Comments

Management's actions, taken and planned, meet the intent of our recommendation. Management will need to record an estimated date for completing its planned actions in the Joint Audit Management Enterprise System (JAMES), Treasury's audit recommendation tracking system.

Finding 2 Treasury Has Challenges With SF 311 Reporting

ISOO uses data submitted on the SF 311 by Executive branch agencies[23] that handle and generate classified national security information to report statistics in its annual report to the President. Therefore, reliable information is imperative. OSP did not provide ISOO with a complete and accurate count of Treasury's derivative and original classification decisions for fiscal years 2013 through 2015. We previously reported this weakness in our 2013 evaluation.

We performed a mathematical check of the SF 311s that Treasury's Departmental Offices and bureaus submitted to OSP for fiscal years 2013 through 2015 and compared them to the consolidated SF 311s prepared by OSP. The analysis disclosed differences in derivative and original classification decisions reported to ISOO. Derivative classification decisions reported on Treasury's consolidated SF 311 to ISOO were different from the sum of the Departmental Offices' and bureaus' reports. An OSP representative could not explain the differences between the sum of component SF 311s and the total on the consolidated SF 311 reported to ISOO. Table 1 provides an analysis of derivative classification differences reported on the SF 311s.

[22] 32 C.F.R. § 2001.23(a)(2), *Classified National Security Information*, states that classified national security information in the electronic environment shall be marked with proper classification markings to the extent that such marking is practical, including portion marking, overall classification, and the classification authority block.

[23] Treasury's Departmental Offices and bureaus are required to provide their SF 311 to OSP by November 1st of each year for inclusion in Treasury's consolidated SF 311 report to ISOO. The Treasury consolidated SF 311 report is submitted to ISOO by November 15th.

Table 1. Reported SF 311 Derivative Classification Decision Differences

Fiscal Year	Office/Bureau Reported SF 311 Decisions	OSP-Prepared Consolidated SF 311 Decisions	Difference
2013	145,428	145,558	130
2014	146,005	145,792	(213)
2015	144,421	147,785	3,364

Source: OIG summary of SF 311s for fiscal years 2013 through 2015

In addition to differences in reported derivative classification decisions, differences also exist between original classification decisions reported on Treasury's consolidated SF 311 and those on Departmental Offices' and bureaus' reports. OSP reported zero original classification decisions for fiscal year 2013, 10 for fiscal year 2014, and 30 for fiscal year 2015. However, when we verified the count with internally submitted data from Treasury Departmental Offices and bureaus to OSP, one office reported 14 original classification decisions for fiscal year 2013, 10 for fiscal year 2014, and 30 for fiscal year 2015. Also, because the number of original classification decisions reported for fiscal year 2015 was relatively high compared to previous years' counts, we reviewed the submitted SF 311s for these years and discussed the differences with the submitting office and OSP.

The submitting office representative confirmed that some of the decisions reported as original classification decisions should have been reported as derivative classification decisions and told us that the other decisions were likely derivative classification decisions as well. The OSP representative also told us that OSP did not question the original classification decisions reported by the submitting office, but acknowledged that they should have been reviewed. The OSP representative also said that OSP experienced significant employee turnover between 2013 and 2015. In addition, we found that Treasury does not have procedures requiring OSP to ensure that Departmental Offices' and bureaus' SF 311s are submitted, and are complete and accurate. The combination of staff turnover and the lack of procedures may have contributed to the inaccuracies.

Recommendations

We recommend that the Assistant Secretary for Intelligence and Analysis direct the Deputy Assistant Secretary for Security to do the following:

1. Update the *Treasury Security Manual* to include OSP responsibilities to (i) follow-up timely with Departmental Offices and bureaus on their SF 311 submissions; (ii) review the SF 311s for completeness and accuracy; (iii) implement a mechanism such as a checklist or reconciliation to ensure complete and accurate reporting of SF 311 information; and (iv) document explanations for corrections made to the Departmental Offices' and bureaus' SF 311 reporting if OSP makes any changes.

   Management Comments

   OSP is reviewing and updating the *Treasury Security Manual* to clarify OSP's responsibilities with respect to SF 311 reporting. As part of this process, OSP is providing more guidance to and communication with Departmental Offices and bureaus through periodic email reminders; will implement a checklist to ensure completeness and accuracy of the reports; will provide one-on-one security assistance to SF 311 action offices; and will document explanations for any corrections made to the SF 311 reports. OSP will also institute additional protocols upon receiving notice of any original classification decisions, and will keep records of those decisions.

2. Provide additional guidance and training to SF 311 preparers focusing on areas of repeated weaknesses such as difficulties identifying the difference between original and derivative classification decisions; and remind the Departmental Offices and bureaus of their responsibilities to ensure that the SF 311 is complete and accurate.

   Management Comments

   OSP has developed a detailed instructional tally sheet to record the Departmental Offices' and bureaus' SF 311 original and

derivative classification decisions for randomly selected cleared individuals. OSP has also provided examples to Departmental Offices and bureaus to demonstrate calculation of classification decisions for SF 311 reporting. In addition, OSP has issued precise guidance to Departmental Offices and bureaus regarding their reporting responsibilities to ensure that each SF 311 report is complete and accurate.

OIG Comments

Management's actions, taken and planned, meet the intent of our recommendations. Management will need to record an estimated date for completing its planned actions in JAMES.

Finding 3 Treasury's Self-Inspection Process Needs Improvement

According to the *Treasury Security Manual,* the annual self-inspection process is a key control to ensure the protection of classified information.[24] Treasury Departmental Offices and bureaus that generate classified information must conduct at least one self-inspection per year, which includes:

- reviewing original and derivative classified decisions;
- stating whether reviewed records, documents, briefings, and activities complied with E.O. 13526 and applicable implementing directives;
- identifying noted discrepancies and indicating whether corrective action will be or has been taken;
- documenting findings and recommendations for improvements or enhancements;
- reporting the results to the OSP Director; and
- conducting and documenting follow-up actions taken where self-inspections have identified such a particular need.

In its role as manager of Treasury's classified program, OSP monitors bureau compliance with the self-inspection requirements.[25] For fiscal years 2013 through 2015, three Treasury bureaus that generate classified information completed the required

[24] TD P 15-71 Chapter III, Section 21, *Self-Inspection Program for Safeguarding Classified Information, Evaluating Security Practices, Procedures and Security Education* (Dec. 30, 2013).
[25] TD P 15-71 *General Information*, *Treasury and Bureau Responsibilities.*

self-inspections, but one bureau did not retain the documentation. In addition, one other bureau did not complete the self-inspection and informed OSP that it believed completing the SF 311 met the requirements for self-inspections. None of these bureaus provided the self-inspection results to OSP nor did OSP request such results.

In 2013, Treasury updated the *Treasury Security Manual* and required bureau self-inspection reporting to the Director of OSP. However, the policy did not include procedures for OSP to follow-up on the self-inspection reports. An OSP representative told us that she was not working for Treasury in fiscal years 2013 and 2014 and did not know why OSP did not have copies of the bureaus' self-inspection results. For fiscal year 2015, the OSP representative told us that OSP did not follow-up on the reports because time was dedicated to the Treasury Security Oversight and Assessment Program.[26] For fiscal year 2016, OSP reminded the bureaus to conduct and report their self-inspection results to OSP.

Self-inspection identifies vulnerabilities and gives Treasury assurance that information security programs comply with requirements and employees understand program requirements. When bureaus do not conduct self-inspections, noncompliance with the information security program relating to the protection of classified information may exist and not be detected. Such systemic vulnerabilities could lead to either inappropriate release or inappropriate restriction of classified information. Requiring OSP to follow-up on outstanding reports would assist in assuring that the required inspections are completed timely.

[26] The Treasury Security Oversight and Assessment Program is a collaborative process designed to assess the effectiveness of security policies in the operational environment and support program improvement of the bureaus. The program reviews security practices using staff visits to bureau headquarters and security operations. These oversight visits will help to clarify guidance to bureau officials, strengthen the *Treasury Security Manual*, and identify and disseminate best practices and lessons learned.

Recommendations

We recommend that the Assistant Secretary for Intelligence and Analysis direct the Deputy Assistant Secretary for Security to do the following:

1. Emphasize to bureaus with employees who handle and generate classified information the importance of conducting annual self-inspections, documenting the results, and submitting the reports to OSP.

   Management Comments

   OSP has disseminated formal email notices to bureaus to remind them of their responsibility under the *Treasury Security Manual* to conduct at least one annual self-inspection, document findings of the inspection, and submit reports to the Director of OSP by October 15th of each calendar year. OSP has implemented a periodic email reminder system to closely monitor this requirement and ensure that it receives self-inspection reports from impacted components.

2. Update the *Treasury Security Manual* to include procedures requiring OSP to follow-up and obtain all bureau self-inspection reports.

   Management Comments

   OSP is in the process of updating the *Treasury Security Manual* to include procedures requiring OSP to follow-up and obtain all bureau self-inspection reports and to clarify the Office of Special Security Program's role in the self-inspection process. OSP will review and update self-inspection procedures for both physical and information security inspections in the *Treasury Security Manual* to reflect best practices.

   OIG Comments

   Management's actions, taken and planned, meet the intent of our recommendations. Management will need to record an estimated date for completing its planned actions in JAMES.

Finding 4 OSP's Training Program Documentation Needs Improvement

According to 32 C.F.R. § 2001.70, *Security Education and Training,* the senior agency official is responsible for the security education and training programs.[27] Each agency must maintain records of training programs, provide annual refresher training with a focus on keeping employees current on established security policies and relevant events, and provide biennial training on the proper application of derivative classification principles. As required by the *Treasury Security Manual,* persons who apply derivative classification markings should be trained in the proper application of derivative classification principles and the training should include identification and required markings; security classification guides; the handling, processing, safeguarding, and destruction of classified information; and information sharing.[28]

The *Treasury Security Manual* requires that all employees with access to classified information receive training in accordance with their level of access and duties.[29] Furthermore, the manual assigns OSP the responsibility for developing security training programs, including the annual refresher training and the derivative classification training, for offices and bureaus.[30, 31] OSP uses different tools to deliver the information, including live group sessions, awareness posters, flyers, notifications and briefings on Treasury's unclassified intranet, *The Green,*[32] and computer-based training modules on TLMS. OSP is also responsible for monitoring Treasury's compliance with required training.

We found that OSP classification training materials were outdated and documentation of training was not consistently maintained. We reviewed documents on *The Green* and found that 14 of the 30

[27] Treasury Order 105-19 designated the Deputy Assistant Secretary for Security as the senior agency official. The Deputy Assistant Secretary has oversight responsibilities for OSP.
[28] TD P 15-71 Chapter III, Section 2, *Mandatory Security Awareness Training* (May 15, 2014).
[29] Ibid
[30] Ibid
[31] TD P 15-71 *General Information, Treasury and Bureau Responsibilities* (June 17, 2011)
[32] *The Green* is Treasury's intranet website providing employees with, among other things, news, announcements, training, policies, directives, and forms.

security education and training documents referenced outdated authorities and/or provided instructions or information that is no longer valid. For example, E.O. 12958 is referenced in several training modules even though it was rescinded by E.O. 13526 in 2009. In addition, 18 security training modules have not been updated since 2010. We also found incorrect marking instructions included in recently updated training materials prepared by OSP.

We also found that OSP did not maintain training records for fiscal years 2013 through 2015 to support completion rates reported to ISOO in the self-inspection documents. For the derivative classification training, Treasury reported completion rates of 46 percent for fiscal year 2013, 63 percent for fiscal year 2014, and 83 percent for fiscal year 2015 in the self-inspection results. When we asked for documentation for the completed training rates, an OSP representative told us that records were not formally maintained and that OSP used email responses to two OSP employees as completion records. The records for these years were not retrievable when we initially requested the documentation because the OSP representatives who received the training completion responses no longer worked for Treasury. An OSP representative later told us that OSP had the ability to retrieve old emails. The 2015 email records of completed training were retrieved but did not support the completion rate reported. Furthermore, Treasury reported 100 percent completion for the required OCA training in fiscal year 2014 to ISOO. However, documents we reviewed disclosed that OSP did not have OCA training records for 9 of the 13 OCA holders in fiscal year 2014.

Since training materials are outdated and documentation of the completion of training is not consistently maintained, OSP cannot be sure that all employees receive the training required by law. An employee who does not receive the required training is more likely to either make errors in classification or improperly classify or mark decisions.

Recommendations

We recommend that the Assistant Secretary for Intelligence and Analysis direct the Deputy Assistant Secretary for Security to do the following:

1. Ensure that training materials are periodically reviewed and updated to include current Federal and Treasury requirements.

   Management Comments

   OSP is currently reviewing and updating all developed security modules, annual security refresher training, and security poster reminders, in accordance with E.O. 13526 and 32 C.F.R. § 2001, to confirm that the most updated security training information is available to Treasury employees. OSP will ensure that the most updated version of the *Treasury Security Manual* is posted on *The Green*.

2. Use TLMS or a similar system to retain records of training and monitor completion of required derivative classifier and original classifier training.

   Management Comments

   OSP is working with TLMS training officials to provide initial information security orientation training and annual security refresher training, which includes both original and derivative classifier training, and additional security related topics, on TLMS. OSP has also taken additional steps to develop a mass email distribution contact list for the cleared employees within Departmental Offices to disseminate security education and training information, and to track annual refresher training. Finally, OSP provides in-person OCA training for all Treasury OCAs and records and retains OCAs' acknowledgement correspondence of completed training.

   OIG Comments

   Management's actions, taken and planned, meet the intent of our recommendations. Management will need to record an estimated date for completing its planned actions in JAMES.

* * * * * *

We appreciate the courtesies and cooperation extended by your staff as we inquired about these matters. Major contributors to this report are listed in appendix 3. A distribution list for this report is provided as appendix 4. If you wish to discuss this report, you may contact me at (202) 927-5904.

/s/
Kieu Rubb
Audit Director

In accordance with Section 6(b) of Public Law 111-258, *Reducing Over-Classification Act,* (the Act) we conducted an evaluation of the Department of the Treasury's (Treasury) classification program to (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within Treasury; and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to the persistent misclassification of material within Treasury. The Act calls for two evaluations. The first evaluation was completed in 2013 and the second evaluation is required to be completed by September 30, 2016.

As required by the Act, we coordinated our evaluation with other Offices of Inspector General with the intent of ensuring that our evaluations followed a consistent methodology to allow for cross-agency comparisons. In performing our work, we used applicable portions of an evaluation guide that was prepared by the working group of participating Offices of Inspector General on behalf of the Council of the Inspectors General on Integrity and Efficiency.

To accomplish our objectives, we performed the following actions.

- Reviewed federal and Treasury rules, regulations, policies, and procedures, including:
    - Executive Order 13526, *Classified National Security Information* (Dec. 29, 2009);
    - 32 C.F.R. § 2001, *Classified National Security Information* (June 28, 2010) ;
    - Public Law 111-258, *Reducing Over-Classification Act* (Oct. 7, 2010);
    - *Treasury Security Manual*, Treasury Directive Publication 15-71 (June 20, 2014); and
    - Treasury Order 105-19, *Delegation of Original Classification Authority; Requirements for Downgrading and Declassification* (June 27, 2011).
- Interviewed the Deputy Assistant Secretary for Security and employees from the Office of Security Programs (OSP) and the Office of Special Security Programs who are responsible for directing and guiding the protection of personnel,

information, facilities, and assets; and for promoting security awareness within Treasury.

- Interviewed a non-statistical sample of Treasury derivative classifiers who are responsible for classifying and portion marking classified decisions selected for review and Departmental Office's personnel responsible for completing the SF 311.
- Reviewed training materials posted on Treasury's unclassified intranet, *The Green,* and paper copies of training documents.
- Reviewed fiscal years 2013 to 2015 training records for Treasury officials with original classification authority.
- Reviewed OSP's and bureaus' self-inspection reports for fiscal years 2013 to 2015.
- Reviewed Treasury's SF 311s prepared by OSP for fiscal years 2013 to 2015, and related data on original and derivative classification decisions provided to OSP by Departmental Offices and bureaus.
- Reviewed a non-statistical sample of 108 derivative classification decisions selected from the 147,785 derivative classification decisions reported on Treasury's consolidated SF 311 for fiscal year 2015. The population reported on Treasury's consolidated SF 311 included emails, reports, official correspondence, memoranda, and presentations. Our sample consisted of 71 emails and 37 non-emails and was selected for the purpose of obtaining a cross-section of Treasury offices and bureaus and types of decisions. The sample was not selected for the purpose of projecting an error rate to the population, and as such, we do not make a projection.
- To select our sample we:
    - Obtained an understanding of the total population of derivative classification decisions on the consolidated SF 311 that Treasury submitted to ISOO for fiscal year 2015. Compared this consolidated SF 311 to the individual SF 311s that Departmental Offices and bureaus submitted to OSP for fiscal year 2015 and determined

which offices reported the majority of the derivative classification decisions.

- Interviewed representatives from three of the offices reporting to the Under Secretary for Terrorism and Financial Intelligence which reported the majority of the derivative classification decisions. These interviews allowed us to gain an understanding of the type of derivative classification decisions prepared and where the decisions are maintained.
- Selected derivative classification decisions from the three offices that prepared 95 percent of the classification decisions reported on Treasury's consolidated SF 311 for fiscal year 2015. The Office of Terrorism and Financial Intelligence (TFI) employees that we interviewed estimated that approximately 70 percent of derivative classification decisions were emails and 30 percent were non-emails. Therefore, we selected our sample to include 71 emails and 37 non-emails to be representative of the universe. We reviewed 71 classified emails from six TFI employees. For each of the six employees, we reviewed all of their sent classified emails from three days. We chose three days in an attempt to get one or more decisions from each person selected, but to avoid an excessive amount from any one person. We selected 37 non-emails from the three offices by selecting different types of classification decisions that each office produces.

We conducted fieldwork in Washington, DC, at the offices reporting to the Under Secretary for Terrorism and Financial Intelligence. Our evaluation scope covered the period from October 2012 to September 2015 and did not include the Internal Revenue Service.[33] We conducted our fieldwork from November 2015 through June 2016.

We conducted this evaluation in accordance with Quality Standards for Inspections and Evaluations issued by the Council of the Inspectors General on Integrity and Efficiency.

[33] The Internal Revenue Service, under the jurisdictional oversight of the Treasury Inspector General for Tax Administration, does not have an individual designated with original classification authority.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

September 16, 2016

MEMORANDUM FOR DEBBIE L. HARKER
ACTING ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: S. LESLIE IRELAND SLI
ASSISTANT SECRETARY FOR INTELLIGENCE AND ANALYSIS

SUBJECT: Management Response to Second Draft Office of the Inspector General (OIG) Report Required by Public Law 111-58, Reducing Over-Classification Act

Thank you for the opportunity to review the Office of Inspector General's (OIG) draft report providing the results of your second evaluation of the Department of the Treasury's (Treasury) classification program, pursuant to Public Law 111-258, *Reducing Over-Classification Act*. As described in Appendix 1 of the OIG's draft report, the scope of this audit reviewed training records, quarterly self-inspection records, and SF 311s for the years 2013-2015. During the time period covered by this audit, OIA management has hired new personnel into the Office of Security Programs (OSP), which is actively working to improve training on classification markings, documentation of training, and SF 311 and self-inspection reporting from the Departmental Offices and Treasury Bureaus. The Office of Intelligence Analysis (OIA) concurs with all of the recommendations and is in the process of implementing many of the OIG's recommendations as outlined below.

Finding 1 Classification Decisions Are Missing Required Markings

Recommendation

We recommend that the Assistant Secretary for Intelligence and Analysis direct the Deputy Assistant Secretary for Security to emphasize to derivative classifiers the importance of properly marking classification decisions, including adding a note in classified emails to remind employees to properly portion mark emails before sending.

Management Response

OSP is coordinating with the Office of Special Security Programs (SSP) to develop a security training campaign which will include training on derivative classification decisions and portion markings. As part of this effort, OSP has already placed updated copies of the Information Security Oversight Office (ISOO) "Marking Classified National Security Information" guide in all of the Sensitive Compartmented Information Facilities (SCIFs) for employee reference purposes. Training on properly marking classification decisions and properly portion-marking emails is routinely provided to employees, both initially when receiving their security clearance for access to classified information and annually during security refresher training (in hard copy and electronic format).

OSP is developing additional comprehensive and tailored training for varied DO/bureau clients to be provided on the Security Program section of Treasury Learning Management System (TLMS). OSP will work closely with DO TLMS officials when developing training modules to ensure that training is accessible in some form to all bureau personnel. All the above referenced training will remind authorized employees of the obligation to properly mark and safeguard classified information.

Additionally, OSP has launched review of marking policy in the Treasury Security Manual, TD P 15-71. With respect to marking electronic media, OSP will determine whether to allow for the same flexibility authorized by the ISOO in its implementing regulation[1].

Finding 2 Treasury Has Challenges With SF 311 Reporting

Recommendations

1. **Update the Treasury Security Manual to include OSP responsibilities to (i) follow-up timely with Departmental Offices and bureaus on their SF 311 submissions, (ii) review the SF 311 for completeness and accuracy, (iii) implement a mechanism such as a checklist or reconciliation to ensure complete and accurate reporting of SF 311 information and (iv) document explanations for corrections made to the Departmental Offices' and bureaus' SF 311 reporting if OSP makes any changes.**

Management Response

OSP is reviewing and updating the Treasury Security Manual to clarify OSP's responsibilities with respect to SF 311 reporting. As part of this process, OSP is providing more guidance to and communication with DO/bureaus that will be submitting SF 311 reports through periodic email reminders to DO/bureau personnel. Once the SF 311 reports are received, OSP will implement a checklist to ensure completeness and accuracy of the reports, provide one-on-one security assistance to SF 311 action offices, and document explanations for any corrections made to the SF 311 reports. OSP will institute additional protocols upon receiving notice of any Original Classification Authority (OCA) decisions, and will keep records of those decisions made by Treasury OCAs.

2. **Provide additional guidance and training to SF 311 preparers focusing on areas of repeated weaknesses such as difficulties identifying the difference between original and derivative classification decisions; and remind Departmental Offices and bureaus of their responsibilities to ensure that the SF 311 is complete and accurate.**

Management Response

OSP has developed a detailed instructional tally sheet to record the DO/bureaus' SF 311 original and derivative classification decisions for randomly selected cleared individuals. OSP has also provided examples to DO/bureaus to demonstrate calculation of classification decisions (original and derivative) for SF 311 reporting. In addition, OSP has issued precise guidance to DO/bureaus regarding their reporting responsibilities to ensure that each SF 311 report is complete and accurate.

[1] 32 CFR Part 2001.23(a)(2), Classified National Security Information, states that classified national security information in the electronic environment shall be marked with proper classification markings to the extent that such marking is practical including portion marking, overall classification, and the classification authority block.

Finding 3 Treasury's Self-Inspection Process Needs Improvement

Recommendations

1. **Emphasize to bureaus with employees who handle and generate classified information the importance of conducting annual self-inspections, documenting results and submitting the reports to OSP.**

Management Response

OSP has disseminated formal email notices to bureaus to remind them of their responsibility under the Treasury Security Manual to conduct at least one annual self-inspection, document findings of the inspection, and submit reports to the Director of OSP by October 15th of each calendar year. OSP has implemented a periodic email reminder system to closely monitor this requirement and ensure that it receives self-inspection reports from all DO/bureaus.

2. **Update the Treasury Security Manual to include procedures requiring OSP to follow-up and obtain all bureau self-inspection reports.**

Management Response

OSP is in the process of updating the Treasury Security Manual to include procedures requiring OSP to follow-up and obtain all bureau self-inspection reports and to clarify SSP's role in the self-inspection process. OSP will review and update self-inspection procedures for both physical and information security inspections in the Treasury Security Manual to reflect best practices.

Finding 4 OSP's Training Program Documentation Needs Improvement

Recommendations

1. **Ensure that training materials are periodically reviewed and updated to include current Federal and Treasury requirements.**

Management Response

OSP is currently reviewing and updating all developed security modules, annual security refresher training, and security poster reminders, in accordance with E.O. 13526 and ISOO Implementing Directive 32 CFR Part 2001, to confirm that the most updated security training information is available to Treasury employees. SSP will similarly review the annual Sensitive Compartmented Information (SCI) training material to confirm that it is updated to include current Federal and Training requirements. OSP will ensure that the most updated version of the Treasury Security Manual is posted on *The Green*.

2. Use TLMS or a similar system to retain records of training and monitor completion of required derivative classifier and original classifier training.

Management Response

OSP is working with TLMS training officials to provide initial information security orientation training and annual security refresher training, which includes both original and derivative classifier training, and additional security related topics, on TLMS. SSP will work with TLMS to track the annual SCI training completion. In addition to providing this training on TLMS, OSP has taken the additional steps of developing a mass email distribution contact list for the cleared employees within DO in order to easily disseminate security education and training information, and to track annual refresher training. The annual refresher training includes derivative classifier training. Finally, OSP provides in-person initial and annual OCA training for Treasury OCAs and records and retains OCAs acknowledgement correspondence of completed training.

Gregory J. Sullivan Jr., Audit Manager
Brigit A. Larsen, Auditor-in-Charge
Regina A. Morrison, Auditor
Allison N. Jackson, Program Analyst
John K. Snyder, Auditor
Richard J. Wood, Referencer

Department of the Treasury

Secretary of the Treasury
Deputy Secretary
Under Secretary for Terrorism and Financial Intelligence
Deputy Assistant Secretary for Security
Director, Office of Security Programs
Office of Strategic Planning and Performance Management
Office of the Deputy Chief Financial Officer, Risk and Control Group

Information Security Oversight Office

Director

Office of Management and Budget

OIG Budget Examiner

United States Senate

Chairman and Ranking Member
Committee on Homeland Security and Government Affairs

Chairman and Vice Chairman
Select Committee on Intelligence

Chairman and Ranking Member
Committee on Finance

Chairman and Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations

U.S. House of Representatives

Chairman and Ranking Member
Committee on Homeland Security

Chairman and Ranking Member
Permanent Select Committee on Intelligence

Chairman and Ranking Member
Committee on Oversight and Government Reform

Chairman and Ranking Member
Committee on Financial Services

Chairman and Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations

THIS PAGE INTENTIONALLY LEFT BLANK

Treasury OIG Website

Access Treasury OIG reports and other information online:
http://www.treasury.gov/about/organizational-structure/ig/Pages/default.aspx

Report Waste, Fraud, and Abuse

OIG Hotline for Treasury Programs and Operations – Call toll free: 1-800-359-3898
Gulf Coast Restoration Hotline – Call toll free: 1-855-584.GULF (4853)
Email: Hotline@oig.treas.gov
Submit a complaint using our online form:
https://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx