OFFICE OF THE SECRETARY

Classified Information Policies and Practices at the Department of Commerce Need Improvement

FINAL REPORT NO. OIG-13-031-A

SEPTEMBER 30, 2013

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

For Public Release

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

September 30, 2013

MEMORANDUM FOR: Thomas R. Predmore
Director, Office of Security

FROM: Andrew Katsaros
Assistant Inspector General for Audit

SUBJECT: *Classified Information Policies and Practices at the Department of Commerce Need Improvement*
Final Report No. OIG-13-031-A

Attached please find the final report of our audit to promote the accurate classification of information. Our audit objectives were to (a) assess whether the Department's applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered, and (b) identify what policies, procedures, rules, regulations, and management practices may be contributing to the misclassification of material.

We found that the Department had generally adopted policies, procedures, rules, and regulations prescribed by Executive Order 13526, "Classified National Security Information." However, we identified areas where the Department could improve certain classification policies, procedures, rules, and regulations prescribed by order 13526 and the Department's *Security Manual*. Our report details how (a) the Department must ensure its policies and practices are consistent with federal requirements and (b) oversight and internal control processes need improvement.

We have received your September 27 response to our draft report. Where appropriate, we have modified this final report based on this response. The formal Office of Security response is included as an appendix. The final report will be posted on the OIG's website pursuant to section 8L of the Inspector General Act of 1978, as amended.

In accordance with the Department Administrative Order 213-5, within 60 days of the date of this memorandum, please provide us with an action plan that responds to all of the report recommendations.

We would like to express our thanks to your staff for the courtesies shown to us during our review. Please direct any inquiries regarding this report to me at (202) 482-7859—or Mark Zabarsky, Audit Director, at (202) 482-3884—and refer to the report title in all correspondence.

Attachment

Report In Brief

SEPTEMBER 30, 2013

Background

Executive Order (order) 13526, "Classified National Security Information" prescribes a uniform system effective June 27, 2010, for classifying, safeguarding, and declassifying national security information. In addition to controlling the amount and duration of classification and sharing classified information more freely, order 13526 outlines mandatory training requirements for those with classification authority.

The Department of Commerce is responsible for both implementing national policies and establishing Departmental policies to ensure that such information is adequately safeguarded when necessary and appropriately shared whenever possible. Within the Department, the Director of the Office of Security is responsible for overseeing all security management. The Department has been proactively reducing the number of classified documents.

Why We Did This Review

The Reducing Over-Classification Act of 2010 (Public Law 111-258) mandates that each inspector general with an officer or employee authorized to make original classification decisions conduct two evaluations to promote the accurate classification of information. The first evaluation must be completed by September 30, 2013; a second, to be completed by September 30, 2016, must review progress made after the first. Our audit objectives were to (a) assess whether the Department's applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered, and (b) identify what policies, procedures, rules, regulations, and management practices may be contributing to the misclassification of material.

OFFICE OF THE SECRETARY

Classified Information Policies and Practices at the Department of Commerce Need Improvement

OIG-13-031-A

WHAT WE FOUND

We found that the Department has generally adopted policies, procedures, rules, and regulations prescribed by order 13526. However, we identified areas where the Department could improve certain classification policies, procedures, rules, and regulations:

The Department must ensure its policies and practices are consistent with federal requirements.

Documents are not being received and reviewed timely for declassification or destruction. Our review of 61 classified documents found that 17 of them may have exceeded their declassification date and should have been referred for a declassification review. We found that a Department employee did not take action to request a mandatory declassification review of the documents that might have been inappropriately classified.

Derivative classification documents contained marking deficiencies. We reviewed 40 Department-generated classified documents and found that 15 derivatively generated documents reviewed had marking deficiencies that did not follow order 13526 requirements. These conditions occurred because the Office of Security neither (a) provided adequate biennial training on applying derivative classification markings nor (b) had guidance in place complying with order 13526.

Oversight and internal control processes need improvement.

Data reported in Security Manager were inaccurate. The Office of Security uses the Security Manager database to track and account for the entire Department's classified information. However, for 14 of the 61 documents, we found that the data reported in Security Manager were inaccurate.

Poor inventory practices contributed to inaccurate information. The Office of Security requires that offices maintaining classified information conduct an annual inventory and review of their classified holdings. However, we found that the offices who conducted the inventories could not provide evidence that they performed the inventory as required—and that the approaches these offices used in conducting the reviews were inconsistent.

WHAT WE RECOMMEND

We recommend that the Director, Office of Security:

1. ensure that the document custodian take action to finalize the disposition of the three documents identified with expired declassification dates;
2. require container custodians to be responsible for the classified documents in the container(s) they control;
3. amend the *Security Manual* to align with the language in Executive Order 13526 regarding markings on derivatively classified documents, as well as update biennial training on classification markings for derivatively generated documents;
4. improve the process for entering accurate data into Security Manager and develop guidance addressing the processes to be followed for annual classified information inventory reviews; and
5. incorporate any relevant changes made as a result of recommendations in this report as part of the Office of Security's annual reviews of the Department's classified information.

Contents

Introduction 1
Objectives, Findings, and Recommendations 3
I. Department Must Ensure Its Policies and Practices Are Consistent With Federal Requirements 4
A. Documents Did Not Receive Timely Review for Declassification or Destruction 4
B. Derivative Classification Documents Contained Marking Deficiencies 5
II. Oversight and Internal Control Processes Need Improvement 7
A. Data Reported in Security Manager Were Inaccurate 7
B. Poor Inventory Practices Contributed to Inaccurate Information 7
Recommendations 8
Summary of Agency Response and OIG Comments 9
Appendix A: Objectives, Scope, and Methodology 10
Appendix B: Agency Response 12

COVER: Detail of fisheries pediment, U.S. Department of Commerce headquarters, by sculptor James Earle Fraser, 1934

Introduction

Since 1951, executive orders have directed government-wide classification standards and procedures. Executive Order (order) 13526, "Classified National Security Information"—signed by the President on December 29, 2009, and effective June 27, 2010—prescribes a uniform system for classifying, safeguarding, and declassifying national security information. In addition to controlling the amount and duration of classification and sharing classified information more freely among the executive branch and state, local, tribal, and private sector partners, order 13526 outlines mandatory training requirements for those with original and derivative classification authority. Pursuant to order 13526, the Information Security Oversight Office (ISOO)[1] provided a directive stating that training requirements must consist of classification standards, classification levels, classification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

The Reducing Over-Classification Act of 2010 (Public Law 111-258)[2] mandates that the inspector general of each agency of the United States with an officer or employee authorized to make original classification decisions conduct two evaluations to promote the accurate classification of information. The first evaluation must be completed by September 30, 2013; a second evaluation, to be completed by September 30, 2016, must review progress made pursuant to the results of the first. The Act—designed to address the issues highlighted by the National Commission on the Terrorist Acts Upon the United States about overclassification of information and to promote information sharing across the federal government and with state, local, tribal, and private sector entities—states: "[O]ver-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information."

Two significant changes to the classification program resulted from order 13526. First, classified information will be made accessible to the maximum extent possible to authorized holders. Second, classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the recipients meet the criteria for authorized holders. However, the originating agency may restrict dissemination by obtaining approval of the National Archives and Records Administration ISOO or the Director, National Intelligence, as applicable.

The Department of Commerce creates, receives, handles, and stores classified information as part of its mission. As a creator and user of classified information, the Department is responsible for both implementing national policies and establishing Departmental policies to ensure that such information is adequately safeguarded when necessary and appropriately shared whenever possible. With proper classification of classified products, the Department can share more information with external stakeholders. Within the Department, the Director of

[1] ISOO is responsible for policy oversight of the government-wide classification system. According to ISOO policy, the receiving agency must treat the information the same way as original information.

[2] Enacted October 7, 2010.

the Office of Security is responsible for overseeing all security management. The classified information results from original classification by Department officials, documents derived from other source documents, and documents from other agencies.

According to order 13526, information determined to require protection from unauthorized disclosure in order to prevent damage to national security must be marked appropriately to indicate its classification. The expected damage to national security that the original classification authority is able to identify or describe as resulting from unauthorized disclosure determines the classification level:

- *top secret*—exceptionally grave damage,
- *secret*—serious damage, or
- *confidential*—damage.

Further, according to order 13526, no other terms are to be used to identify U.S. classified information, except as otherwise provided by statute. If significant doubt exists about the need to classify or the appropriate level of classification, the information will either not be classified or classified at the lower level.

Only those authorized in writing by the President, the Vice President, agency heads, or other officials designated by the President may originally classify information. These authorities must be trained on proper classification prior to originally classifying information and at least once a year thereafter. *Derivative classification*—the incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material according to the source information—includes the classification of information based on classification guidance. Personnel who apply derivative classification markings must be trained to apply the principles of order 13526 prior to derivatively classifying information and at least once every 2 years thereafter. Information may be derivatively classified from a source document or documents, or by using a classification guide.

Based on information provided by the Office of Security, the Department had more than 42,000 classified documents in 2005. Since then, the Department has been proactively reducing the number of classified documents. The Department presently has 122 security containers that contain more than 4,800 classified documents—about 37,000 documents have either been destroyed or transferred outside the Department. The majority of the Department's classified documents are derivatively classified.

Objectives, Findings, and Recommendations

Our audit objectives were to (a) assess whether the Department's applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered, and (b) identify what policies, procedures, rules, regulations, and management practices may be contributing to the misclassification of material. In this Department-wide audit, out of the 4,842 classified documents, we reviewed a random sample of 61. Forty[3] were Department-generated documents, either original or derivative; as such, the Department had classification authority. The remaining 21 documents were created and given to the Department by outside agencies. Appendix A further details the objectives, scope, and methodology of our audit.

We found that the Department had generally adopted policies, procedures, rules, and regulations prescribed by order 13526. For example, the Department

- reduced the number of original classification authorities from 16 to 3,
- revised the *Manual of Security Policies and Procedures*[4] (*Security Manual*) to include ISOO-recommended changes, and
- updated the annual security education and training program content to include required training of original classification authorities and derivative classifiers.

However, we identified areas where the Department could improve certain classification policies, procedures, rules, and regulations prescribed by order 13526 and the Department (see table 1).

Table I. Summary of Findings by Number of Documents

Bureau	Exceeded Mandated Declassification Date	Potentially Exceeded Classification Date	Contained Marking Deficiencies	Recorded Inaccurately in Security Manager
BIS	0	0	11	14
Office of the Secretary	0	0	3	0
NTIA	3	17	1	0
Total	**3**	**17**	**15**	**14**

Source: OIG

[3] Of the 40 documents, 30 were generated derivatively and 10 were original classification.

[4] The *Security Manual*, dated December 2012, establishes security policies and provides procedural guidance for the effective administration of security programs in the Department. Its provisions apply to all Departmental operating units, offices, facilities, employees, contractors and associates, and others who have access to Departmental facilities, information, personnel, or information technology systems.

First, we found that Department employees need to be more proactive in challenging classified documents that either exceeded or may have exceeded declassification dates and should have been referred to the originating agency for a declassification review. In addition, we found that 15 documents had marking deficiencies in one or more of the required elements, such as missing information on the classifier.

Further, we identified areas for which the Department could improve certain classification policies and practices prescribed by the *Security Manual*. For instance, although the Office of Security uses the Security Manager database to track and account for the entire Department's classified information, we found that data reported in Security Manager for 14 documents were inaccurate and incomplete. These inaccuracies highlight the need for improved control procedures to ensure that classified information is properly accounted for and recorded in Security Manager.

Department policy also requires that offices maintaining classified information conduct an annual inventory and review of their classified holdings. However, we found that these offices could not provide evidence of performing these inventories. The deficiencies identified in this audit indicate that the inventories are not properly conducted. Reliable inventory reviews ensure detection of possible documents in the custodians' possession that require downgrade, declassification, or destruction. Finally, we found that the Office of Security did not include adequate biennial training for derivative classifiers on how to apply derivative classification markings on documents.

Without improvements, the weaknesses identified may limit the Department's ability to make informed risk-based decisions that support the protection of classified information and the system on which it resides. As such, we have made several recommendations that, if fully implemented, should help enhance the Department's management of risk of overclassified information.

I. Department Must Ensure Its Policies and Practices Are Consistent With Federal Requirements

The Department has generally adopted—but, in certain cases of classification, does not effectively follow and administer—policies, procedures, rules, and regulations prescribed by order 13526. Specifically, we found that

- documents are not being received and reviewed timely for declassification or destruction and
- derivative classification documents contained marking deficiencies.

A. Documents Did Not Receive Timely Review for Declassification or Destruction

Our review of 61 classified documents found that 17 documents, created and given to the Department by an outside agency, may have exceeded their declassification date and should have been referred to the originating agency for a declassification review. Department officials stated that authorized holders of information (including holders outside the classifying organization) who believe that a classification is improper are to

request a mandatory declassification review (MDR) by the originating agency or originating classification authority.

However, we found that a Department employee did not take action to request this MDR for classified documents that were held beyond the specified date that would trigger such a review. A discussion with the employee who served as custodian for the 17 documents indicated that they were no longer being used or needed by Department staff and could be potentially destroyed or declassified (i.e., sent for a declassification review). Fifteen of these documents were 19–45 years old (2 documents were not dated). Of the 15 dated documents, 12 showed declassification dates ranging between 1993 through 1995. This could result in maintaining documents that could be made available for public release, unnecessarily limiting disclosure and public access. Office of Security personnel reported progress on encouraging Department staff to take action to downgrade or destroy old or unneeded documents. However, the Office of Security needs to continue communicating to employees the importance of forwarding documents that have reached their declassification date for referral to the originating agency or authority for declassification guidance.

In addition, we identified three derivatively classified documents that recently exceeded their mandatory declassification date—March 2012—and should have been referred to the originating agency for a declassification review. We brought this issue to the attention of the document custodian, who was not aware that the declassification date had expired. Although the custodian has contacted the outside agency, resolution regarding the declassification of these documents has not yet taken place. These examples by themselves do not indicate a systemic problem but may suggest that other documents can run the same risk of exceeding their mandated declassification dates, warranting improved agency management of this process. Failing to take timely action to declassify documents could prevent federal agencies from sharing information internally, with other agencies, and with state and local law enforcement, making it more difficult to draw connections and anticipate threats.

B. Derivative Classification Documents Contained Marking Deficiencies

Order 13526 sets forth the specific conditions that must be met when making classification decisions and outlines the procedures to properly mark and classify documents. Derivative classifiers must identify themselves by name and position or personal identifier, as well as observe original classification decisions and carry forward the pertinent markings. Order 13526 also states that persons who apply derivative classification markings shall receive training in the proper application of principles, with an emphasis on avoiding overclassification, at least once every 2 years. We reviewed all 40 Department-generated classified documents and found that 15 derivatively generated documents reviewed had marking deficiencies that were not in compliance with the required document marking elements contained in order 13526 (see table 2).

Table 2. Summary of Findings Documents with Marking Deficiencies

Classification Criteria	Number of Marking Deficiencies	Number of Documents That Could Not Be Verified
Derivative classifier is identified by name and position or personal identifier	10	0
Derivative classifier observed and respected original classification	2	0
For a document derived from multiple sources, the derivative classifier carried forward date or event that corresponds to longest period of classification among the sources	1	7
Derivative classifier attached a listing of classified sources	10	0
Total	**23**[a]	**7**

Source: OIG

[a] We identified a total of 15 documents that contained the 23 deficiencies.

For example, 10 were missing information on the classifier. Not naming the classifier could call into question whether the individual had the proper authority to classify the document. Further, order 13526 states that, in the event of multiple sources, the derivative classifier will carry forward the date or event for declassification that corresponds to the longest period of classification among the sources and list all the source materials. For 7 documents, we could not verify the declassification date because the source documents were not available or the source was not identified.

These conditions occurred because the Office of Security neither

- provided adequate biennial training for personnel responsible for applying derivative classification markings, nor
- had guidance in place complying with order 13526 requiring the name and position or personal identifier to be listed on the derivatively classified document.

Order 13526 requires that derivative classifiers receive training at least once every 2 years, with an emphasis on avoiding overclassification. However, we found that the Office of Security did not include adequate training for derivative classifiers on how to apply derivative classification markings on documents. On June 13, 2013, we brought this matter to the attention of the Office of Security. Subsequently, an Office of Security representative stated that they revised their training course to include applying derivative classification markings for sessions beginning in FY 2014.

If employees with derivative classification authority do not receive proper guidance and training on policies and procedures, classified documents, or portions of classified

documents, may be improperly released; the authors of classified documents may be unknown; and employees may not have all of the information necessary for declassification.

II. Oversight and Internal Control Processes Need Improvement

The Office of Security could improve certain classification policies and practices prescribed in its *Security Manual*. Effective program management includes reliable information systems, a comprehensive inspection program, and comprehensive training for classifiers. Specifically, we found that

- data reported in Security Manager were inaccurate and
- poor inventory practices contributed to inaccurate information.

A. Data Reported in Security Manager Were Inaccurate

The *Security Manual* requires document classifiers to maintain records in Security Manager concerning original and derivative classification actions. The Office of Security uses the Security Manager database—for which the Department has established procedures to ensure accurate data input—to track and account for the entire Department's classified information. Servicing security offices[5] or security contacts[6] are required to review records and reports to ensure the information submitted by document classifiers is complete and accurate. Furthermore, as part of its yearly document inspection program, the Office of Security verifies the accuracy of information input into Security Manager. However, for 14 of the 61 documents, we found that the data reported in Security Manager were inaccurate. For example, 12 documents had been destroyed but Security Manager showed them as still in the inventory. In another example, Security Manager showed that 1 document was located in the District of Columbia when in fact it had been transferred to an office in California in July 2008.

These inaccuracies highlight the need for improved control procedures to ensure that classified information is properly safeguarded, accounted for, and recorded in Security Manager. Maintaining accurate data is an essential component of good oversight and helps lead to informed decisions.

B. Poor Inventory Practices Contributed to Inaccurate Information

The *Security Manual* requires that offices maintaining classified information conduct an annual inventory and review of their classified holdings, stating that (a) each document must be visually inspected during the annual inventory to ensure it is complete or

[5] *Servicing security offices* implement and monitor compliance with Departmental security program activities in bureaus, operating units, and Departmental offices under their jurisdiction.

[6] A *security contact* is appointed by Departmental organizations to serve as a liaison to the Office of Security to address all matters of security.

accounted for and (b) inventory results should be forwarded to the responsible office's security contact. However, we found that the offices who conducted the inventories could not provide evidence that they performed the inventory as required—and that the approaches these offices used in conducting the reviews were inconsistent. For example, even though one office stated that it had performed the reviews, it had neither documented nor reported the results. Another office stated that it had randomly selected documents for review but verbally provided confirmation of their results to the responsible office's security contact. Even though these offices stated reviews are being performed, the deficiencies found in this report (e.g., three documents that had declassification dates went unnoticed for more than a year; the disposition of destroyed documents was not properly recorded in Security Manager) indicate that the inventories are not properly conducted. The lack of specific guidance contributed to the inconsistent approaches among the offices concerning how to perform their annual inventory reviews. Reliable inventory reviews ensure detection of possible documents in the custodians' possession that require downgrade, declassification, or destruction.

Recommendations

We recommend that the Director, Office of Security:

1. ensure that the document custodian take action to finalize the disposition of the three documents identified in the audit with expired declassification dates;

2. require container custodians to be responsible for the classified documents in the container(s) they control and (a) promote and enforce user reviews of classified documents, as well as (b) ensure custodians are trained and understand their responsibilities to account for, control, and purge classified materials;

3. amend the *Security Manual* to align with the language in Executive Order 13526 that requires the name and position or personal identifier to be listed on derivatively classified documents, as well as update biennial training to include how to apply classification markings on derivatively generated documents;

4. improve the process for entering accurate data into Security Manager and develop guidance addressing the processes to be followed to conduct and document annual classified information inventory reviews; and

5. incorporate any relevant changes made as a result of recommendations in this report as part of the Office of Security's annual reviews of the Department's classified information.

Summary of Agency Response and OIG Comments

OIG received the Department's comments on the draft report, which we include as appendix B of this final report. Based on the Department's review of the draft and subsequent discussions with our office, we have made some changes to the language in the report. The Department concurs with the findings and recommendations in the report.

Appendix A: Objectives, Scope, and Methodology

The objectives of our audit were to (a) assess whether the Department's applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered, and (b) identify what policies, procedures, rules, regulations, and management practices may be contributing to the misclassification of material.

To accomplish our objectives, we obtained a list from the Department's Office of Security to identify the population of classified documents. The Office of Security's list was generated from the Security Manager data system, covering classified documents as of April 4, 2013. Initially, we judgmentally selected 74 out of 4,842 classified documents for review. However, we were not able to test 13 documents we intended to include in our audit because 12 documents had been destroyed and 1 was transferred to another location outside the DC metro area. Consequently, we sampled 61documents—40 of which were Department of Commerce generated and the remaining 21 were created and given to the Department by outside agencies. Top secret documents were not included within the scope of our audit of classified documents due to the process necessary to access these records and the availability of properly cleared staff.

In addition, we

- discussed management classification practices with the Office of Security and the four regional offices (National Institute of Standards and Technology Security Office, Gaithersburg, MD; Western Regional Security Office, Seattle, WA; Census Bureau Security Office, Suitland, MD; and National Oceanic and Atmospheric Administration Security Office, Silver Spring, MD);

- compared the Department's *Security Manual* policies with those required by Executive Order (order)13526;

- evaluated the Department's management practices used to list and track the classified documents and to train all staff that has the ability to derivatively classify documents;

- evaluated the Office of Security's internal controls; and

- coordinated our scope and methodologies with the other agency inspectors general.

Further, we obtained an understanding of the internal controls by evaluating Office of Security responses to the statement of assurance for FYs 2011and 2012 and by interviewing Office of Security staff and assessing their adherence to the requirements in order 13526 and the Department of Commerce *Manual of Security Policies and Procedures*. While we identified and reported on internal control deficiencies, no incidents of fraud, illegal acts, violations, or abuse were detected within our audit. We found weaknesses in the Department's controls related to (a) its inadequate action and annual statement of assurance responses and (b) the processes and

procedures used to originally and derivatively classify documents and correctly maintain and inventory the documents in its classified containers.

We tested the reliability of the data provided in the Security Manager system by analyzing it for irregularities and inconsistencies such as missing data, misstatements, and other obvious errors. However, we did not have access to the IT system. While we noted discrepancies, they were not a material representation of the entire population of information and, thus, we consider the system data sufficiently reliable for use in our audit.

We conducted the audit fieldwork between March 2013 and August 2013. We performed our fieldwork at the Department of Commerce, Office of Security and their regional offices at the Census Bureau, Suitland, Maryland; the National Institute of Standards and Technology, Gaithersburg, Maryland; and the National Oceanic and Atmospheric Administration in Silver Spring, Maryland.

We performed our work under the authority of the Inspector General Act of 1978, as amended, and Department Organizational Order 10-13, August 31, 2006. We conducted this audit 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.

Appendix B: Agency Response

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

SEP 27 2013

MEMORANDUM FOR Andrew Katsaros
Assistant Inspector General for Audit

FROM: Thomas Predmore
Director of Security
Office of Security

SUBJECT: Response to Draft Report: Classified Information Policies and Practices at the Department of Commerce Need Improvement

Thank you for the opportunity to review and respond to the draft report for the classification policies and practices at the DOC. Concurrence is provided for the "Recommendations" suggested.

1. **Ensure that the document custodian take action to finalize the disposition of the three documents identified in the audit with expired declassification dates.**
   a. OSY will obtain document identifiers from OIG Team to determine custodian, and provide instructions for referral of documents for mandatory declassification review.
   b. OSY will provide focus on mandatory declassification in the initial and refresher national security information briefings.
2. **Require container custodians to be responsible for the classified documents in the container(s) they control and (a) promote and enforce user reviews of classified documents, as well as (b) ensure custodians are trained and understand their responsibilities to account for, control, and purge classified materials.**
   a. OSY will provide one-on-one training to container custodians on the proper control of classified documents.
   b. OSY will improve its pre-inspection checklist so that custodians better understand the responsibility to (a) enforce user reviews of classified documents for declassification and marking; and (b) improve custodian knowledge for controlling and purging classified documents.
3. **Amend the Security Manual to align with the language in Executive Order 13526 that requires the name and position or personal identifier to be listed on derivatively classified documents, as well as update annual refresher training to include how to apply classification markings on derivatively generated documents**
   a. Security Manual will be updated in accordance with the Executive Order and the ISOO Marking Guide.
   b. Refresher training will be updated to better describe the process of applying proper derivative classification markings.

4. **Improve the process for entering accurate data into Security Manager and develop guidance addressing the process to be followed to conduct and document annual classified information inventory reviews**
    a. OSY will train custodians on the requirement for inventorying and complying with the Security Manual.
    b. Security Manual will be updated to include the requirement to report inventories to the OSY.
    c. OSY will provide a copy of documents listed in Security Manager, to each custodian for the annual inventory. The custodian will use the Security Manager data as their report back to OSY for reconciliation and compliance.
5. **Incorporate any relevant changes made as a result of recommendations in this report as part of the Office of Security's annual reviews of the Department's classified information.**
    a. OSY reviews security containers on a recurring basis, and will implement recommendations from this review, with documentation for deficiencies and corrective actions.

Again, I appreciate the opportunity to make formal and informal comments to the draft report, and look forward to working with you to address the items of concern, provided herein. We thank you for supporting the Information Security Program, and we will work to address all the items you provide in your recommendations and the final report.

If you have any questions or concerns, please contact Eric Dorsey, Assistant Director for Counterespionage, at (202) 482-1266.

011200000160