Office of Inspector General

July 25, 2014

MEMORANDUM

TO: SEC, Director of Security, Mark Webb

FROM: IG/A/PA, Director, Jon Chasson /s/

SUBJECT: Evaluation of USAID's Implementation of Executive Order 13526, Classified National Security Information (Report No. 9-000-14-002-S)

This memorandum transmits our final report on the subject evaluation. In finalizing the report, we considered your comments on the draft evaluation and have included them in Appendix II.

The report contains 11 recommendations to help strengthen the implementation of USAID's classified national security program. We acknowledge your management decisions on all the recommendations and final action on 4 and 6. Please provide the Audit Performance and Compliance Division with the necessary documentation to achieve final action on the other recommendations.

Thank you and your staff for the support and courtesies extended to us during this evaluation.

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20523
http://oig.usaid.gov

SUMMARY

The Reducing Over-Classification Act, Public Law 111-258, was enacted in October 2010 to prevent overclassification of information and to promote sharing information within the Federal Government, with state and local government, and with the private sector. It followed President Barack Obama's December 2009 Executive Order 13526, "Classified National Security Information," which "prescribes a uniform system for classifying, safeguarding and declassifying national security information." According to the order, "Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of standards and routine, secure, and effective declassification are equally important priorities."

Section 6 of the Act, "Promotion of Accurate Classification of Information," includes the following requirement for Office of Inspector General (OIG) evaluations:

> [T]he inspector general of each department or agency of the United States with an officer or employee who is authorized to make original classifications, in consultation with the Information Security Oversight Office, shall carry out no less than two evaluations of that department or agency or a component of the department or agency
>
> (A) to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and
>
> (B) to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency or component.

This requirement applies to USAID because the Agency has four positions with original classification authority (OCA) up to the secret level. There are two types of classifications—original and derivative. According to USAID's policy glossary, original classification involves making an "initial determination that information requires, in the interest of national security, protection against unauthorized disclosure," and derivative classification involves "reproducing, extracting, or summarizing classified information, or applying classification markings derived from source material or as directed by a classification guide." All of the approximately 2,600 USAID employees with a security clearance have derivative classification authority.

This is the first of two OIG evaluations responding to the act. We used the guide for conducting evaluations developed by the Department of Defense OIG.[1] In accordance with the act, we conducted the evaluation in consultation with the Information Security Oversight Office (ISOO), part of the National Archives and Records Administration that is responsible to the President for policy and oversight of the U.S. Government's security classification system.

USAID's primary policy for implementing the order is Automated Directives System (ADS) 568, "National Security Information Program," maintained by the Agency's Office of Security. The

[1] *A Standard User's Guide for Inspectors General Conducting Evaluations under Public Law 111-258, the "Reducing Over-Classification Act,"* January 22, 2013.

director of that office reports annually to the director of ISOO and is responsible for confirming that USAID implements the order.

ADS 568 delegates responsibility for maintaining a system of accounting for top-secret information to USAID's Executive Secretary. For USAID missions, the Embassy's regional security officer is responsible for the security programs. USAID missions may not store classified information and must process classified information in the Embassy.

OIG's Performance Audits Division conducted this evaluation. The objectives were to:

1. Assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within USAID; and

2. Identify policies, procedures, rules, regulations or management practices that may be contributing to persistent misclassification of material within USAID.

USAID's classification policy (ADS 568) generally meets the requirements set forth in the order, but it needs updating to reflect current practice. In addition, USAID has not published a classification guide.[2] In response to the second objective, we did not find evidence of persistent misclassification of material within USAID. However, we did find other problems, listed below.

- USAID reported incorrect classification statistics (page 4). Agencies with OCA are required to report classification statistics to ISOO each year. USAID sampled staff on how many classification decisions they performed over a 2-week period and projected from the sample to estimate how many of each type of classification (confidential, secret, or top secret) were made for the year; however, we found errors in USAID's calculations.

- USAID's self-inspection program did not include representative samples of classified documents (page 5). In addition, the security office had not reviewed classified documents from the electronic network.

- Classified documents were marked incorrectly (page 6). Although none of the 21 documents in our sample was overclassified, only 5 were marked correctly.

- USAID did not issue a classification guide or update parts of the classification policy (page 7). The order requires agencies to develop their own classification guide, but USAID currently uses the State Department's.

- Agency staff did not receive guidance on the ClassNet marking tool (page 8). For e-mailing and processing confidential and secret information, USAID uses ClassNet, an electronic network with service provided by the State Department. ClassNet users said they would like more guidance on how to use the marking tool.

- OCAs did not receive customized training (page 9). USAID only offers a combined training for derivative and original classifiers.

[2] ADS 568 states that a classification guide is "a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element."

To address these problems and strengthen USAID policies and procedures for classified information, we recommend the Office of Security:

1. Develop, implement, and document a sampling method for reporting classification decisions that can be projected to the total population of classifiers at USAID (page 5).

2. Train employees who are required to report information on classification decisions to make sure they understand their reporting duties, and document such training (page 5).

3. Update ADS 568 to state that inspections of classified documents shall be conducted using a representative sample (page 6).

4. Conduct inspections of classified information using a formal process with a representative sample, and document the results of the testing (page 6).

5. Implement a procedure to work with the Chief Information Office during inspections to sample users of the electronic system (ClassNet) and test for overclassification and classification markings (page 6).

6. Identify documents marked incorrectly during inspections and explain proper marking to employees performing the classifications, and document the results (page 7).

7. Identify employees who perform a large quantity of derivative classifications, and enforce proper management of classified information by including it as an element in their performance evaluations (page 7).

8. Publish USAID's classification guide during fiscal year 2014 (page 8).

9. Update ADS 568 to reflect the Agency's current requirements for employees recording classification decisions (page 8).

10. Work with the Chief Information Office to train ClassNet users on how to use the marking tool, and document such training (page 9).

11. Provide customized OCA training annually to original classifiers, and document that they have completed the training (page 9).

Detailed findings follow. The evaluation's scope and methodology appear in Appendix I. Management comments appear in their entirety in Appendix II, and our evaluation of them is on page 10 of the final report.

EVALUATION RESULTS

USAID Reported Incorrect Classification Statistics

Executive Order 13526 and its implementing directive, 32 Code of Federal Regulations Part 2001, require agencies to report annual statistics on their security classification programs using Standard Form 311, "Agency Security Classification Management Program Data," to ISOO. The director of ISOO tells agencies what statistics should be included in their reporting.

ISOO guidelines state, "Actual counts of classification decisions for a 52-week period are always preferred, but for many large agencies this may not be practical," thus allowing agencies to use a sampling technique if they determine it is impractical to provide actual counts of top-secret, secret, and confidential derivative classification decisions. USAID decided to use ISOO's sampling technique, and we confirmed with ISOO that agencies have discretion over their sampling methodology. This includes defining the population, sample number, and duration.

The Agency did not report any original classifications from 2010 through 2013. Table 1 shows the number of derivative classifications USAID reported.

Table 1. Derivative Classifications Reported to ISOO (Unaudited)

Year	Top Secret	Secret	Confidential	Total
2010	0	0	0	0
2011	10	195	14	219
2012	0	312	104	416
2013	208	494	208	910

We found errors in the number of derivative decisions reported to ISOO. In 2013 the Office of Security sampled 20 percent of Agency staff on how many classification decisions they performed over a 2-week period. The office intended to project that information to the entire Agency for the course of the year by multiplying by 5 and 26, respectively.[3] However, employees in that office did not use the multiplier (5) to project to the total population, leading to an incorrectly calculated estimate of classified decisions for 2013. They also did not document how the sample and population were determined.

We spoke with administrative management specialists (AMSs) and administrative assistants tasked with providing classification statistics to the Office of Security for USAID's 2013 reporting to ISOO.[4] Several said they did not understand the tasks they were required to perform. For example, one AMS confused derivative classification authority with OCA. She said her office does not produce classified information because it does not have the authority to do so. However, all USAID employees with a security clearance have derivative classification authority,

[3] According to ISOO, a derivative classification count of a 20 percent sample population is multiplied by 5 to project to the total population (100 percent). Because the sample captures data for a 2-week period, the count is multiplied by 26 to get the full year classification count.

[4] To collect information on classification decisions, the Office of Security sends a PowerPoint document to AMSs with reporting instructions. In it, AMSs are asked to collect information over a 2-week period.

and we reviewed derivatively classified documents from that office, which means it performs derivative classification decisions.

One administrative assistant reported four top-secret derivatively classified decisions to the Office of Security. When asked by the evaluation team who classified these documents, she said the documents were provided to her office by USAID's Office of the Executive Secretariat and were classified by other agencies. She said she misunderstood what was being asked and had reported to the Office of Security the number of documents that her office received, not the number her office derivatively classified. This error led to over-reporting the Agency's top-secret derivative classifications in 2013.

Security officials agreed that using ISOO guidance not tailored to a USAID-specific sampling method and population led to incorrect reporting of classification statistics. While the office provided a PowerPoint document to teach AMSs on how to report classification decisions, some of them did not understood what was required.

Without a well-documented sampling method for reporting classification decisions and correct classification decision data, the Office of Security is at risk of continuing to provide inaccurate statistics to ISOO on the Agency's security classification program.

> ***Recommendation 1.*** *We recommend that the Office of Security develop, implement, and document a sampling method for reporting classification decisions that can be projected to the total population of classifiers at USAID.*
>
> ***Recommendation 2.*** *We recommend that the Office of Security train employees who are required to report information on classification decisions to make sure they understand their reporting duties, and document such training.*

Self-Inspection Program Did Not Include Representative Samples of Classified Documents

The order states that agencies shall establish and maintain a self-inspection program and report results annually to the ISOO director. One of the program's activities is to conduct "regular reviews of representative samples of their original and derivative classification actions."

The Office of Security does not use a representative sample when reviewing classified material, and it does not keep a log of any marking errors. Instead, three security specialists perform random inspections of bureaus/independent offices (B/IOs) at USAID. They look at a random number of classified documents in each office safe, but they do not document how many safes or documents they review.

Additionally, most of USAID's classification actions occur in ClassNet, but Office of Security employees do not review information in the system. As a result, they do not review most of the Agency's original and derivative classification actions.

Security officials agreed that the process of reviewing classified documents should be more formal, and they developed a template to be used in future inspections. Additionally, because USAID does not create a significant amount of classified information, inspection findings focused on activity and security container checklists not being completed or retained, missing

signs to indicate copiers and shredders are not authorized for classified documents, and improperly stored safe combinations instead of whether documents were classified correctly. Checking whether classified materials are marked appropriately could be useful for identifying trends and weaknesses in training.

The officials said they asked the Office of the Chief Information Officer (CIO) for access to review e-mails in the State Department's ClassNet system but were not able to get it. They reported this in the 2011, 2012, and 2013 reports to ISOO. State Department officials confirmed there is no way to separate USAID e-mails from State Department e-mails in ClassNet.

Because there is no formal documentation or process for the Office of Security's self-inspections of classified documents, we could not verify compliance with this component of the order. Furthermore, because the majority of classified documents at USAID are classified derivatively using ClassNet and the Office of Security is not reviewing that system, it is not aware whether information is being overclassified or mismarked.

> ***Recommendation 3.*** *We recommend that the Office of Security update Automated Directives System 568 to state that inspections of classified documents shall be conducted using a representative sample.*
>
> ***Recommendation 4.*** *We recommend that the Office of Security conduct inspections of classified information using a formal process with a representative sample, and document the results of the testing.*
>
> ***Recommendation 5.*** *We recommend that the Office of Security implement a procedure to work with the Chief Information Office during inspections to sample users of the electronic system (ClassNet) and test for overclassification and classification markings.*

Classified Documents Were Marked Incorrectly

The order states that people who derivatively classify information shall:

- Be identified by name and position.
- Include all classification markings in any newly created document.
- Identify the source document or classification guide.
- Reprint the "declassify on" line from the source document.
- Clearly mark materials with the highest classification level of information contained in it.
- Mark each portion of a derivatively classified document immediately before the portion it applies to.

Additionally, the order states that personnel who regularly apply derivative classification markings be evaluated in their performance rating on their designation and management of classified information.

As part of the evaluation, 21 documents from 5 B/IOs within USAID were reviewed. None of the 21 documents were overclassified. However, several were marked with only the classification level, making it difficult to evaluate the appropriateness of the classification, and only five reviewed had correct markings. We found the following marking errors.

- 12 documents did not include the source the document was derived from.
- 12 documents did not include the duration of the classification.
- 10 documents did not have markings before each portion of the document.
- 4 documents did not have proper overall markings.

During the course of the evaluation, we noticed several other drafts of classified documents—not selected in our sample or included in the counts above—that were missing appropriate markings.

Some employees who performed the derivative classifications in the sample were not sure of what constituted a derivative classification. Others said they do not regularly perform derivative classifications as part of their job. However, everyone interviewed had attended the classification or annual refresher trainings and was informed on how to mark classified materials correctly.

Because there are no consequences for incorrect classification markings, employees have little incentive to mark documents accurately. Office of Security officials said they have been working with the Office of Human Resources to put language into staff performance evaluations regarding classification and marking procedures.

When documents—even in draft form—are not marked correctly, the classified status of information and level of protection required is unknown. There is a possibility that documents could be distributed improperly to people without a need to know, or that people will overclassify improperly marked documents as a precautionary measure. Improper safeguarding is a threat to national security, and overclassification prohibits the sharing of information.

> ***Recommendation 6.*** *We recommend that the Office of Security identify documents marked incorrectly during inspections and explain proper marking to employees performing the classifications, and document the results.*
>
> ***Recommendation 7.*** *We recommend that the Office of Security identify employees who perform a large quantity of derivative classifications, and enforce proper management of classified information by including it as an element in their performance evaluations.*

USAID Did Not Issue Classification Guide or Update Parts of Classification Policy

The order requires agencies with OCA to develop classification guides. USAID, however, did not, and it currently uses the State Department's guide. Office of Security officials said they have been drafting a guide for more than 3 years and intend to release it in 2014. They said they had not published the guide yet because of changes in management and competing priorities.

USAID's primary guidance on implementing the order is ADS 568. This guidance generally meets the requirements set forth in the order, but it needs to be updated to adjust sections no longer applicable. For example, the ADS states:

- AMSs for the Administrator, Deputy Administrator, and Inspector General must maintain a log of all classified decisions made annually.

- B/IOs must maintain a centralized log of all classification activity.

- All employees who derivatively or originally classify documents must maintain an unclassified record of those activities.

Security officials said USAID employees are no longer required to maintain the logs and that the requirement was applicable when most classified information was processed on paper rather than electronically.

Therefore, until ADS 568 is updated, USAID staff will continue to use guidance no longer deemed applicable by the Office of Security. The Agency will not be compliant with the order's requirements and will continue to make classification decisions based on the State Department's guidance until a USAID-specific guide is published.

> ***Recommendation 8.*** *We recommend that the Office of Security publish USAID's classification guide during fiscal year 2014.*
>
> ***Recommendation 9.*** *We recommend that the Office of Security update Automated Directives System 568 to reflect the Agency's current requirements for employees recording classification decisions.*

Agency Staff Did Not Receive Guidance on ClassNet Marking Tool

The order mandates USAID to establish and maintain a security education and training program. ADS 568.3.4 states the training program will ensure that employees are aware of their responsibilities concerning classified information such the procedures for classification, marking, control, storage, transmission, and destruction.

Agency employees use ClassNet to e-mail and process confidential and secret information. The service provider for ClassNet is the State Department. According to the Office of the CIO, USAID/Washington has approximately 120 ClassNet terminals and about 450 user accounts.

Employees who need to access ClassNet must undergo training, which consists of CIO's cyber-awareness training and Office of Security's training. We spoke with 14 USAID employees who regularly use ClassNet. Some said they used the marking tool recently for classifying e-mails and added that they would like more guidance on using it. They also gave suggestions such as providing a tutorial, including the tool in security training, e-mailing a guide to ClassNet users, or offering a drop-down menu with options.

CIO staff said the ClassNet marking tool was deployed only on updated terminals; consequently, not all employees have seen it. Security officials said they would work with CIO to train employees how to use the tool.

Because the majority of classifications are performed electronically, it is important that system users are trained adequately to mark electronic documents, including e-mails and attachments. If users do not use the marking tool correctly, information may not be controlled or transmitted appropriately.

> ***Recommendation 10.*** *We recommend that Office of Security work with the Chief Information Office to train ClassNet users on how to use the marking tool, and document such training.*

Original Classification Authorities Did Not Receive Customized Training

The order states, "All original classification authorities must receive training in proper classification . . . at least once a calendar year." Furthermore, ADS 568.3.4.4 states that the Office of Security "will provide training for all OCAs"—implying this training is unique. Both the order and ADS 568 require derivative classifiers to receive training at least once every 2 years.

The training program that the Office of Security provides meets the requirements outlined in the order. To verify compliance, the office uses a computer system to track employees' training.

We verified the records for 17 employees with derivative classification authority, and all had completed training within 2 years. However, we found that not all OCAs completed their training within 1 year.

While conducting the sample, two documents were found from fiscal years 2011 and 2012 that were prepared by an OCA, with "reason" for the classification in the marking block. This indicates the documents were originally classified; if they were derivatively classified, they would have had "source" in the marking block. However, these documents were not reported to the Office of Security and therefore not reported to ISOO during the annual reporting process, as required.[5]

The Office of Security's current training program is for both original and derivative classifiers. Security officials recognized the need for specific OCA training, and the office developed a module to address those requirements during our evaluation.

If OCAs do not receive specific training on their duties and responsibilities, there is a greater potential for overclassification. Additionally, they may continue to make original classifications without informing the Office of Security. This affects the accuracy of the classification decisions reported to ISOO. It also makes it difficult for the office to review original classification decisions and verify that OCAs are classifying and safeguarding information appropriately.

> ***Recommendation 11.*** *We recommend that the Office of Security provide customized original classification authority training annually to original classifiers, and document they have completed the training.*

[5] The annual reporting process is explained on page 4 of this report.

EVALUATION OF MANAGEMENT COMMENTS

In their comments on the draft evaluation report, agency officials agreed with all 11 recommendations, and we acknowledge management decisions on all of them.[6] Based on our review of management's comments and supporting documentation, we agree that final action has been taken on Recommendations 4 and 6. A detailed evaluation of management comments follows.

Recommendation 1. The Office of Security updated and documented the sampling methodology for completing ISOO reporting requirements. Final action requires that the office implement the updated methodology during the next ISOO reporting period, which staff said is in October 2014.

Recommendation 2. Officials in the Office of Security said they plan to train AMSs responsible for completing Standard Form 311, used to report classification statistics annually to ISOO. Final action requires that AMSs receive training and that the training is documented. The Office of Security expects final action to be completed by September 2014.

Recommendation 3. The Office of Security provided draft revisions of ADS 568 stating that items covered during the security inspection program would include representative sampling of original and derivative classification actions. Final action requires issuing the updated ADS, which the Office of Security expects will be completed by October 30, 2014.

Recommendation 4. The Office of Security updated the process for inspecting classified documents and documented results for B/IOs tested in May and June 2014. Based on the comments and supporting documentation provided, we acknowledge that the office made a management decision and that final action has been taken.

Recommendation 5. The Office of Security updated its sampling procedures to meet ISOO reporting requirements, and it developed a classification action log for Agency staff to report classification actions they performed in ClassNet. Final action requires that the office implement a procedure for testing for overclassification and classification markings in ClassNet.

Recommendation 6. The Office of Security updated its procedures for inspecting safes, providing corrective training to staff whom improperly marked documents, and documenting the training. Based on the comments and supporting documentation of May and June 2014 inspections, we acknowledge that the office made a management decision and that final action has been taken.

Recommendation 7. The Office of Security coordinated with the Office of Human Resources and proposed language to include in annual performance evaluations for USAID employees who routinely create or handle classified information. Final action requires that the appraisals include this new performance element, and the office expects final action to be completed by

[6] The draft evaluation report dated May 27, 2014, contained 14 recommendations. Due to revisions of 12 FAM 530, three of these recommendations were no longer relevant and were removed from the final report.

January 1, 2015.

Recommendation 8. The Office of Security drafted a security classification guide and provided it to ISOO for review and comment. Final action requires that the guide is issued, which the office expects would be done by September 30, 2014.

Recommendation 9. The Office of Security drafted revisions to ADS 568 to reflect USAID's requirements for employees recording classification decisions. Final action requires that the updated ADS 568 be issued, which the office expects would be done by September 30, 2014.

Recommendation 10. Office of Security officials said they are coordinating with the CIO and State Department on deploying ClassNet training. Final action requires that ClassNet users receive training and that training is documented, which the office expects would be completed by December 30, 2014.

Recommendation 11. The Office of Security developed an OCA training package. Final action requires the OCAs complete the training and that the training is documented, which the office expects would be completed by September 30, 2014.

SCOPE AND METHODOLOGY

Scope

OIG's Performance Audits Division carried out this evaluation in response to a mandate in the Reducing Over-Classification Act. We believe our work on this evaluation fulfills that mandate. The evaluation was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency's 2012 *Quality Standards for Inspection and Evaluation*.

Fieldwork was performed in Washington, D.C., from February 5 to April 3, 2014. OIG reviewed classification management policies and practices within USAID, including those developed internally, and assessed whether existing procedures are appropriate to make sure that classified national security information is classified and marked properly.

The evaluation covered the period from June 2010 to April 2014. This report is directed to Office of Security staff responsible for the Agency's implementation of Executive Order 13526.

Methodology

To plan for this evaluation, we reviewed the Reducing Over-Classification Act, Executive Order 13526, ISOO guidance for implementing the order, applicable regulations, and relevant OIG work. We also reviewed USAID's National Security Information Program policy and external reporting, internal inspections, and self-assessments pertaining to classification requirements. To compare USAID to other agencies, we conducted this evaluation using the Department of Defense's *A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the "Reducing Over-Classification Act*."

During fieldwork, we interviewed staff from the Office of Security, Office of the Executive Secretariat, and Office of the CIO responsible for implementing the order, maintaining accountability of classified materials, and verifying that Agency personnel with classification authority are compliant with training requirements. We interviewed 14 employees who performed derivative classifications or have authority to do so. We interviewed AMSs who have classification reporting duties. We reviewed the Office of Security's reports to ISOO and the supporting data used to report statistics on the Agency's classification program. To test training, we compared requirements mandated by the order to USAID guidance and training materials. We also tested 20 employees' training records to determine whether they were current on training requirements.

For this evaluation, we did not review classified e-mails in ClassNet or JWICS or SCI documents maintained in the SCIFs. Instead, we reviewed paper documents. To sample classified materials, we selected seven B/IOs with the aim of reviewing five documents in each B/IO. However, in some B/IOs we found fewer than five, and two B/IOs did not have any classified paper documents for the team to review. Overall, we reviewed 21 classified documents in five B/IOs. Additionally, classified documents in USAID's two SCIFs were reviewed with the support of Office of Security and Office of the Executive Secretariat staff. The two SCIF reviews did not identify any top-secret materials classified by USAID employees.

We judgmentally selected the 21 classified documents because USAID does not have a universe, or log of classified materials that could be used for statistical sampling. Therefore, the evaluation results cannot be projected to the entire population. The evaluation team entered each B/IO, moving from safe to safe with the assistance of the AMS until at least five documents were reviewed or the team determined five paper documents were not available.

MANAGEMENT COMMENTS

July 7, 2014

MEMORANDUM

TO: IG/A/PA, Martha Chang, Acting Director

FROM: SEC/OD, Mark Webb, Director of Security /s/

SUBJECT: Office of Inspector General Evaluation of USAID's Implementation of Executive Order 13526, Classified National Security Information (Report No. 9-000-14-00X-S).

Thank you for affording USAID Office of Security (SEC) with an opportunity to respond to the draft audit of USAID's Implementation of Executive Order (E.O.) 13526. SEC has reviewed the draft audit findings and recommendations and we are working diligently to address the weaknesses identified in the report. SEC reached management decisions on all 14 recommendations. Recommendations to 5 of the 14, specifically 1, 4, 5, 6 and 11, have been fully implemented. We have responded to 9 of the 14 recommendations outlined in the draft OIG report dated May 27, 2014 by taking the following actions:

1. RECOMMENDATION: Develop, implement, and document a sampling method for reporting classification decisions that can be projected to the total population of classifiers at USAID.

- RESPONSE: SEC agrees with this recommendation. Standard Operating Procedures have been developed and implemented which include a specific sampling methodology for completing the SF-311 that is consistent with the Information Security Oversight Office (ISOO) guidance for original and derivative classification reporting. OIG auditors reviewed the SOP and SEC requests that this recommendation be closed.

2. RECOMMENDATION: Train employees who are required to report information on classification decisions to make sure they understand their reporting duties, and document such training.

- RESPONSE: SEC agrees with this recommendation. Although training had been provided to AMS Officers on the completion of the SF-311 form, it was determined they did not understand the requirements of this task. A training curriculum has been developed for completing the SF-311. SEC will provide training to AMS Officers responsible for completing the SF-311 report by September 30th of each year (anticipating the report is due to ISOO on/about October 30). The completed training will be made part of the official training records.

3. RECOMMENDATION: Update ADS 568 to state that inspections of classified documents shall be conducted using a representative sample.

- RESPONSE: SEC agrees with the recommendation. Agency policy has been drafted to include a representative sampling of classification actions for original and derivative classification and is pending for the clearance process. OIG auditors reviewed this draft and agreed that once published this recommendation could be closed. Target completion date for official publication is October 30, 2014.

4. RECOMMENDATION: Conduct inspections of classified information using a formal process with a representative sample, and document the results of the testing.

- RESPONSE: SEC agrees with the recommendation. Standard Operating Procedures (SOPs) have been revised to include conducting a representative sampling of original and derivative classified documents from all safes during the inspection period. All final inspection reports will include the findings. The SOP has been reviewed by OIG auditors, and SEC requests this recommendation be closed.

5. RECOMMENDATION: Implement a procedure to work with the Chief Information Office (CIO) during inspections to sample users of the electronic system (ClassNet) and test for over-classification and classification markings.

- RESPONSE: SEC agrees with this recommendation. Self-Inspection Program SOPs have been revised to also include methodology for a representative sampling of classification actions performed on Information Technology systems. OIG auditors have reviewed this SOP and SEC requests this recommendation be closed.

6. RECOMMENDATION: Identify documents marked incorrectly during inspections and explain proper marking to employees performing the classifications, and document the results.

- RESPONSE: SEC agrees with this recommendation. A review of classified documents is now conducted during the annual inspection period; findings are reported in the final inspection report. Training will be provided within 30 days to USAID employees that have incorrectly marked documents. The inspection SOP has been updated to reflect this change. OIG auditors have reviewed this SOP and SEC requests this recommendation be closed.

7. RECOMMENDATION: Identify employees who perform a large quantity of derivative classifications, and enforce proper management of classified information by including this duty as an element in their performance evaluations.

- RESPONSE: SEC concurs with this recommendation. SEC has coordinated the requirement and proposed language be incorporated as a critical performance element in annual performance appraisals with the Office of Human Resources (OHR). SEC is currently waiting for approval from OHR. The target completion date is January 1, 2015.

8. RECOMMENDATION: Publish USAID's classification guide during fiscal year 2014.

- RESPONSE: SEC concurs with the recommendation. The draft Security Classification Guide was provided to ISOO on June 20, 2014 for review and comment before final publication. SEC anticipates incorporating ISOO comments/suggestions and publishing the final SCG by September 30, 2014.

9. RECOMMENDATION: Update ADS 568 to reflect the Agency's current requirements for employees recording classification decisions.

- RESPONSE: SEC concurs with this recommendation. Agency policy has been drafted and is pending SEC Management approval prior to being sent for Agency clearance. Target completion date is September 30, 2014.

10. RECOMMENDATION: Require TSCOs and alternate TSCOs are designated, and document the designations.

- RESPONSE: 12 FAM 530 which established the authority and policy requirements for the TSCO was rescinded effective October 1, 2013, thus removing general TSCO policy guidance and requirements. Agency policy changes to remove all references to TSCO have been drafted and are pending the clearance process for formal publication. The target completion date is September 1, 2014.

11. RECOMMENDATION: Develop training for TSCOs, and document and track training compliance in accordance with Agency policies.

- RESPONSE: 12 FAM 530 which established the authority and policy requirements for the TSCO was rescinded effective October 1, 2013, thus removing general TSCO policy guidance and requirements. SEC requests this recommendation be closed.

12. RECOMMENDATION: Work with the Office of the Executive Secretariat (ES) to implement standard operating procedures that account for reproductions of classified documents in accordance with the Foreign Affairs Manual.

- RESPONSE: SEC agrees with this recommendation. SEC will collaborate with ES to develop a SCIF SOP outlining internal control measures to adequately safeguard TS material. The target completion date is August 1, 2014.

13. RECOMMENDATION: Work with the Chief Information Office to train ClassNet users on how to use the marking tool, and document such training.

- RESPONSE: SEC agrees with this recommendation. Although SEC provides initial and annual training on the proper markings for classified documents, additional training for the ClassNet (now Thin Client) automated marking tool may be required. SEC will

coordinate with CIO on strategies to deploy training on the marking tool. Coordination and collaboration between SEC, CIO and the Department of State is currently underway to address this recommendation. The target completion date is December 30, 2014.

14. RECOMMENDATION: Provide customized OCA training annually to original classifiers, and document they have completed the training.

- RESPONSE: SEC agrees with this recommendation. An OCA training package has been developed. The four USAID OCAs will receive OCA training and completion will be made part of the official training records. The target completion date is September 30, 2014.

If you have questions about the responses, please feel free to contact Kim Bazemore at (202) 712-1374, or email: kbazemore@usaid.gov.

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20523
Tel: 202-712-1150
Fax: 202-216-3047
http://oig.usaid.gov