OFFICE OF INSPECTOR GENERAL

USAID'S IMPLEMENTATION OF EXECUTIVE ORDER 13526, CLASSIFIED NATIONAL SECURITY INFORMATION, NEEDS SIGNIFICANT IMPROVEMENT

AUDIT REPORT NO. 9-000-16-001-P
SEPTEMBER 30, 2016

WASHINGTON, DC

Office of Inspector General

September 30, 2016

MEMORANDUM

TO: Deputy Administrator, Ambassador Alfonso E. Lenhardt

FROM: Assistant Inspector General for Audit, Thomas E. Yatsco /s/

SUBJECT: USAID's Implementation of Executive Order 13526, Classified National Security Information, Needs Significant Improvement (9-000-16-001-P)

This memorandum transmits our final report on the subject audit. The objectives were to (1) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material at USAID, (2) assess whether applicable classification policies, procedures, rules, and regulations—including Executive Order 13526—have been adopted, followed, and effectively administered at USAID, and (3) determine whether USAID addressed recommendations OIG made in our July 2014 report. In finalizing the audit report, we considered your comments on the draft and included them in their entirety in appendix II.

The audit report contains one recommendation to help strengthen USAID's classified national security information program. We acknowledge your management decision on the recommendation.

We appreciate the cooperation and assistance extended to us during this audit.

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

INTRODUCTION

The Reducing Over-Classification Act, Public Law 111-258, was enacted in October 2010 to prevent overclassification of information and to promote information sharing within the Federal Government; with State, local, and tribal entities; 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."

The act requires inspectors general to carry out and report on at least two evaluations of their agencies' compliance with classification policies, procedures, rules, and regulations. This audit is the second of the two required reports by the USAID Office of Inspector General (OIG). We issued the first, "Evaluation of USAID's Implementation of Executive Order 13526, Classified National Security Information" (9-000-14-002-S), on July 25, 2014.

OIG conducted this audit to do the following:

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

2. Assess whether applicable classification policies, procedures, rules, and regulations—including Executive Order 13526—have been adopted, followed, and effectively administered at USAID.

3. Determine whether USAID addressed recommendations OIG made in our July 2014 report.

To conduct our work, we reviewed Federal and Agency policy and regulations and interviewed Agency officials. We used nonstatistical random samples and other methods to test USAID's compliance with the regulations. In addition, we reviewed corrective actions taken in response to recommendations in our previous report. Additional details about our scope and methodology are in appendix 1. We conducted this audit in accordance with "Government Auditing Standards" as prescribed by the Comptroller General of the United States.

SUMMARY

We concluded that, from October 1, 2014, to June 15, 2016, USAID's one originally classified document was properly classified and contained the required classification markings. Further, our audit did not find evidence of persistent misclassification of derivatively classified information at USAID.

However, we found that USAID's classification policy does not meet the requirements set forth in Executive Order 13526, and the Office of Security has not effectively administered USAID's classified national security information program. We found persistent and systemic noncompliance related to program management, security education and training, self-inspections, the issuance of an Agency classification guide, reporting of program activities and

results to the National Archives and Records Administration's Information Security Oversight Office (ISOO), and classification markings.

Further, USAID's implementation of the 11 recommendations in our 2014 report was incomplete. The Office of Security reported that, as of August 24, 2015, it had made management decisions and taken corrective actions on all 11 recommendations. However, we found that two corrective actions were not implemented, and seven were not implemented effectively to remedy the deficient condition. The recommendations included training employees who have original classification authority, who report on classification decisions, who use ClassNet, and who handle and safeguard classified materials; conducting inspections of classified information using a formal process with a representative sample; and issuing USAID's classification guide. Given the depth, sensitivity, and persistence of the weaknesses we found in operations, reporting, and compliance, we consider them a significant internal control deficiency. USAID has not devoted sufficient management or staff attention to complying with Executive Order 13526 or addressing prior OIG recommendations.

To address these deficiencies and strengthen USAID's policies and procedures, we recommend that the Office of the Administrator implement a corrective action plan, described in the Agency's Automated Directives System (ADS), chapter 596, to bring USAID's classified national security information program into full compliance with Executive Order 13526 and ISOO regulations and directives.

Our evaluation of management comments is on page 11, and the full text of management comments is in appendix II.

BACKGROUND

Executive Order 13526 designates ISOO to issue implementing regulations that agencies must follow, and to oversee agency actions to ensure compliance. ISOO issues Title 32 of the Code of Federal Regulations, Part 2001 (32 CFR 2001), "Classified National Security Information," which establishes standards for classification, declassification, identification and marking, the safeguarding of classified information, self-inspection programs, security education and training, prescribed standard forms, and required reporting.

There are two types of classification: 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." Derivative classification involves "reproducing, extracting, or summarizing classified information, or applying classification markings derived from source material or as directed by a classification guide."[1] Four positions at USAID have the authority to make original classification decisions—i.e., determine that information needs protection and mark it accordingly—up to the Secret level. They are the Administrator, Deputy Administrator, Director of Security, and Inspector General. All USAID employees with a security clearance have derivative classification authority.

[1] Glossary of ADS Terms, partially revised on April 30, 2014.

Our 2014 report found instances of noncompliance in reporting, self-inspections, security trainings, and classification markings and found that USAID had not issued a classification guide. To address these concerns, we made recommendations to update USAID's policy to conform to ISOO guidance, implement representative sampling,[2] develop appropriate trainings, use employees' performance evaluations to enforce proper management and handling of classified information, and issue a classification guide.

AUDIT RESULTS

USAID Properly Classified Its Own Information

We found no evidence of persistent misclassification of information at USAID. From October 1, 2014, to June 15, 2016, USAID's single originally classified document was its classification guide. USAID properly classified this document.

USAID mainly uses information classified by other Federal agencies, including the Departments of State and Defense. For the same period, using a sample of USAID's derivatively classified information, we found no evidence of misclassification at USAID.

USAID's Classified National Security Information Program Does Not Comply With Executive Order 13526 and Information Security Oversight Office Regulations and Directives

We found that USAID was not complying with the order in managing the program, doing security education and training, conducting self-inspections, issuing a classification guide, reporting classified national security information to ISOO, or applying classification markings.

Program Management. Section 5.4 of Executive Order 13526 requires heads of agencies that originate or handle classified information to designate a senior agency official to administer the classified national security information program and direct how information is classified, safeguarded, and declassified. Agency policy designates the Director of the Office of Security as USAID's senior official responsible for promulgating guidance on USAID's classified national security information program.[3] This guidance is issued through ADS chapter 568 for the program's overall policies and procedures, and through ADS chapter 510 for USAID's mandatory declassification review policies and procedures.

Our review of ADS 568 and 510 identified the following deficiencies.

- ADS does not have policies and procedures to implement all Executive Order 13526 and 32 CFR 2001 requirements. For example, it lacks policies and procedures for the following:

    - Conducting systematic declassification reviews.

[2] Given the large number of employees who have derivative classification authority, USAID does not maintain a catalog of derivatively classified documents and emails produced each year. Instead, the Agency chooses to use representative sampling to estimate the actual number.
[3] Automated Directives System 101.3.1.4.

- Conducting a fundamental classification guidance review.
- Prohibiting and limiting classification actions.

- ADS 568 has policies and procedures that do not fully comply with the following requirements of Executive Order 13526 and 32 CFR 2001:

  - Procedures for challenging classification do not state that employees are protected from retribution and do not provide deadlines that USAID must meet for responding to challenges, including appeals.[4]
  - Procedures do not include requirements for reporting self-inspection program results to ISOO.
  - Procedures do not provide for suspension of original classification authority when training requirements are not met.

- ADS chapters 101, 510, 545, 552, 562, 566, and 567 are outdated; they reference the authority of Executive Order 12958 of April 1995, which Executive Order 13526 replaced.

In addition, two individuals in the Bureau for Management responsible for managing USAID's declassification program did not have a Top Secret clearance and could not oversee the work of USAID's declassification expert responsible for declassifying all of USAID's classified information, including Top Secret documents.

Security Education and Training. The Code of Federal Regulations provides requirements for agencies to implement a classified information training program, including who must attend, how often training should occur, and what training materials should cover.[5]

Our review of USAID's compliance with 32 CFR 2001.70 and 71 disclosed the following deficiencies.

- As part of the Office of Security's initial security briefing, employees must sign a nondisclosure agreement (a Standard Form [SF]-312), witnessed and accepted by an Office of Security representative. Yet the forms we reviewed had the following deficiencies:

  - In two cases, witness signatures were dated later than employee signatures.
  - In one case, an employee (a former USAID Administrator) erroneously signed the "acceptance" block of his own SF-312, which is reserved for Office of Security officials, instead of the signature block.
  - In one case, the Office of Security could not find an employee's SF-312 on file.

- The Office of Security's training presentations and briefings did not fully comply with the requirements of 32 CFR 2001.71 in the following ways:

  - The written training presentation for the initial security briefing did not cover criminal, civil, or administrative penalties.

[4] Section 1.8 of the Executive order states that holders of classified information are "expected to challenge the classification of information that they believe is improperly classified or unclassified."
[5] 32 CFR 2001.70 and 71.

- The written presentation for training on original classification authorities did not cover the duration of classification, identification and markings, classification prohibitions and limitations, use of the security classification guide, or information sharing.
- The written presentation for the annual security refresher training did not cover classification prohibitions and limitations, sanctions, or use of the classification guides.
- Termination briefings did not cover penalties for noncompliance or employees' obligation to return all classified documents and materials in their possession.
- The Office of Security did not use standard training materials, permitting instructors to make presentations with differing content.

- The Bureau for Management manages USAID's declassification program but has not implemented a program to train its declassification authorities on their duties and responsibilities within 6 months of assuming their position.

Self-Inspections. The designated senior agency official is responsible for directing and administering the agency's self-inspection program. The purpose of the program is to verify that all of the offices and the agency as a whole are complying with the classified national security information program.[6]

Our review of the Office of Security's self-inspection program and our own reviews of USAID's offices identified the following deficiencies.

- In all 12 of the USAID offices reviewed (self-inspected by the Office of Security and verified through an independent review by our audit team), deficiencies existed in the self-inspections themselves:

  - Two offices—The Office of Security did not have any documentation of the inspections, and did not have final inspection reports available.
  - One office—The Office of Security had documentation of the inspection, but did not have a final inspection report available.
  - No offices—The self-inspections did not include representative sampling, nor did they evaluate declassifications or classified emails for adherence to the timeliness and marking requirements.
  - Five offices—The Office of Security did not indicate whether it checked to see if the office implemented previous recommendations.

- One office did not have a designated unit security officer (USO) to ensure that operations of that office are carried out in accordance with security policy.

- The Office of Security's designated USO, who is responsible for ensuring office compliance with security policies and procedures, is a member of the team conducting the annual self-inspection. This practice creates a conflict of interest and undermines the ability of the Office of Security to perform its self-inspections with integrity and independence.

- One safe containing classified information was not listed on the Office of Security's safe inventory and turned up in an unrestricted area (i.e., an area not permitted to handle classified information); one safe on the inventory could not be located; and three safes were

[6] 32 CFR 2001.60(b).

found in the wrong location. The Office of Security was not aware of these discrepancies before our audit noted them.

Classification Guide. USAID's classification guide, issued in May 2015, does not list a point of contact for questions or provide guide users a mechanism to report needed changes, as the Code of Federal Regulations requires.[7]

Reporting Program Activities and Results to ISOO. The Code of Federal Regulations requires USAID to report its self-inspections and program statistics to ISOO.[8] However, our review of the Office of Security's reports submitted to ISOO for fiscal year 2015 identified the following deficiencies.

- USAID misreported to ISOO its compliance with self-inspection requirements. USAID reported that it inspected all offices during fiscal year 2015, that it did representative sampling of information including classified emails, and that it fully conducted declassification reviews, security education and training reviews, and interviews with users and producers of classified information—but was unable to support these assertions at the conclusion of fieldwork.

- The Office of Security did not accurately report all of USAID's classification statistics as required by ISOO using form SF 311, "Agency Security Classification Management Program Data."

    - It reported erroneous derivative classification activity because its sampling strategy did not comply with ISOO guidance and relied on offices to self-report derivative classifications instead of conducting a centralized survey.
    - USAID's Bureau for Management's Information and Records Division informed the Office of Security that it had reviewed 152,500 pages for systematic declassification; the Office of Security, in turn, included that number in its report to ISOO. However, when we requested documentation to verify this total, division officials said that only approximately 95,000 pages could be supported.

Classification Markings. The Code of Federal Regulations stipulates: "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."[9] To help agencies, the guidance provides instructions on tasks such as completing the classification authority block; declassifying information; and adding portion markings.

Despite this guidance, derivatively classified documents and emails were not properly marked. Our review showed that noncompliance spanned the categories shown in table 1. Portion markings were the category with the most errors (125, or 86 percent of the total). [10]

[7] 32 CFR 2001.15(b) and 15(d)(2).
[8] 32 CFR 2001.90.
[9] 32 CFR 2001, Subpart C, "Identification and Markings."
[10] Portion markings are applied to paragraphs, subjects, titles, graphics, tables, charts, etc. to indicate which are classified and unclassified.

Table 1. Classification Errors by Category

Classified Information Type	Sample Size	Classified Authority Block	Declassification Instruction	Portion Markings	Overall Classification Markings
Originally Classified					
Documents*	1	0	0	0	0
Subtotal	1	0	0	0	0
Derivatively Classified					
Documents	34	22	22	20	11
Emails	110	25	25	105	110
Subtotal	144	47	47	125	121
Total	**145**	**47**	**47**	**125**	**121**
Error Rate		**32%**	**32%**	**86%**	**83%**

* USAID had only one originally classified document during our audit scope.

USAID Has Not Fully Addressed OIG's Prior Recommendations to Improve Management of Classified Information

Our 2014 report on USAID's compliance with Executive Order 13526 made 11 recommendations to strengthen the Agency's policies and procedures for dealing with classified national security information. The Office of Security reported that, as of August 24, 2015, it had made management decisions to close all 11 recommendations and implemented corrective actions for each.[11] However, two corrective actions were not implemented, and seven corrective actions were not implemented effectively to remedy the deficient condition. This indicates a lack of attention by management and staff to compliance with classified information requirements.

Recommendations Not Implemented. Recommendations 5 and 9 were that the Office of Security implement a procedure to sample users of ClassNet for overclassification and classification markings testing, and that it update ADS chapter 568 to reflect USAID's requirements for employees recording classification decisions, respectively.[12] However, the Office of Security had not taken these corrective actions.

Recommendations Not Effectively Implemented. We made seven recommendations in 2014 that had not been effectively implemented.

[11] According to USAID's policy, after OIG issues a final audit report containing recommendations for USAID action, USAID has 6 months to make a management decision, and must make a reasonable effort to implement a corrective action within a year. Final action can be considered to have taken place after USAID has completed all actions detailed in its management decision.

[12] The Classified Network (ClassNet) is a Department of State owned system that extends its service to USAID/Washington. It is a collection of local workstations networked together and connected to remote Classified Servers maintained at the State Department via encrypted circuits that process information up to the Secret level.

- Recommendation 1. We recommended that the Office of Security develop, implement, and document a sampling method for reporting classification decisions that could be projected to the total population of classifiers at USAID. The Office of Security updated ADS 568.3.1.4 to provide policy for performing representative samples of classification actions for SF-311 reporting. However, our review of fiscal year 2015 SF-311 reporting compliance determined that the total population estimate did not include all personnel able to make derivative classification decisions, such as personal service contractors, institutional contractors, individuals made available under interagency agreements, or Fellows.

- Recommendation 2. We recommended that the Office of Security train employees who are required to report on classification decisions, to ensure that they understand their reporting duties, and document such training. The Office of Security updated ADS 568.3.1.4 to provide policy for training administrative management specialists on their duties to help the Office of Security meet its SF-311 reporting requirements. However, our review of fiscal year 2015 SF-311 reporting compliance determined that not all administrative management specialists attended training, and the training material did not include all the duties required of them.

- Recommendation 3. We recommended that the Office of Security update ADS 568 to state that inspections of classified documents shall be conducted using a representative sample. The Office of Security updated ADS 568.3.1.4 to provide policy for performing representative samples of derivative classification decisions for SF-311 reporting. However, our review of fiscal year 2015 SF-311 reporting compliance determined that samples of classified information do not include any in electronic format, like emails.

- Recommendation 4. We recommended that the Office of Security conduct inspections of classified information using a formal process with a representative sample. However, our review of fiscal year 2015 self-inspections determined that six did not include representative samples of originally and derivatively classified documents or electronic documents.

- Recommendation 6. We recommended that the Office of Security identify documents marked incorrectly during inspections, explain proper markings to employees performing the classifications, and document the results. However, our review of fiscal year 2015 self-inspections did not find support that the Office of Security had discussed improper markings with responsible employees because officials had not documented the results.

- Recommendation 10. We recommended that the Office of Security work with the Office of the Chief Information Officer to train ClassNet users on using the ClassNet marking tool and document such training. The Office of Security and Office of the Chief Information Officer implemented “Classified Network Orientation” training, which includes information on using the marking tool and is required for all new ClassNet users. However, our review of classification markings identified numerous errors, indicating that the training provided has not been effective at improving compliance.

- Recommendation 11. We recommended that the Office of Security provide and document attendance of customized, annual training on original classification authority for original classifiers. The Office of Security implemented training on original classification authority and documented attendance for all original classifiers in fiscal year 2015. However, the training material continues to omit important information, such as the duration of classification, identification and markings, classification prohibitions and limitations, use of

the classification guide, and information sharing. For example, the original classifiers need to be properly trained on prohibitions and limitations on classified information so they understand why information should *not* be classified—e.g., to conceal violations of the law or prevent embarrassment to a person.

Lack of USAID Attention to Managing the Classified National Security Information Program. Several factors have contributed to a lax security culture and USAID's ineffective management of classified national security information and insufficient action on our 2014 recommendations.

- Employees do not always take seriously their duties to safeguard classified information. The Office of Security officials stated that employees frequently fail to mark classified information appropriately despite attending training. Previous self-inspections have identified many of the same problems year after year—employees failing to destroy outdated or unused classified documents, instead leaving them in safes.

- Mechanisms to enforce the regulations are lacking. One Office of Security official noted that while employees have language in their annual performance standards requiring them to protect classified information, management does not enforce the requirements.

- Security is decentralized. Office of Security officials said they primarily provide oversight of USOs, who in turn are responsible for day-to-day security administration and compliance in their offices. Office of Security officials described this relationship as a challenge given the frequent turnover and inexperience of USOs.

- Turnover of security staff has been significant. The Office of Security's director and deputy director positions became vacant and were being filled in an acting capacity. The Counter-Terrorism Information and Industrial Security Division chief position was vacated and remained unfilled. The Information and Industrial Security Branch chief position was vacated and filled toward the end of fiscal year 2015; in the same branch two specialists left in early fiscal year 2015 and were not replaced until the end of the fiscal year. This combination of leadership departures and new staff strained the Office of Security's ability to transfer institutional knowledge effectively to maintain adequate oversight of the program.

Given the depth, sensitivity, and persistence of the problems in the program's operations, reporting, and compliance, we consider them a significant internal control deficiency. Accordingly, it is incumbent on USAID's management to identify and address their root cause through a corrective action plan.[13]

[13] Office of Management and Budget, OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," July 2016.

CONCLUSION

Executive Order 13526 and related classified national security information policy are designed to decrease the probability of persons or foreign nations accessing Government-held information without authorization and using it to harm the national security of the United States. Although USAID only originally classified one document in fiscal year 2015, the policies extend to classified information the Agency receives from other agencies and uses in its own documents and communications. Until USAID improves its program management, security education and training, self-inspections, classification guide, reporting to ISOO, and classification markings and adequately implements recommendations from the previous evaluation, it is not in full compliance with Executive Order 13526. USAID leadership also lacks assurance that its employees are adequately safeguarding national security information, nearly all of it classified by other agencies.

An effective classified national security information program requires robust internal controls over operations, reporting, and compliance. However, in addition to the internal control weaknesses in USAID's compliance with Executive Order 13526 and ISOO regulations and directives, we uncovered significant concerns related to the classified national security information program's operations and reporting. Addressing these deficiencies through a comprehensive corrective action plan is the responsibility of management and must be a priority because of the sensitivity of the subject and the weaknesses identified.

RECOMMENDATION

Recommendation 1. *We recommend that the Office of the Administrator implement a corrective action plan, described in Automated Directives System 596, to bring USAID's Classified National Security Information Program into full compliance with Executive Order 13526 and Information Security Oversight Office regulations and directives.*

EVALUATION OF MANAGEMENT COMMENTS

In responding to the draft report, USAID's Deputy Administrator agreed with the recommendation and instructed the Director of the Office of Security to develop a corrective action plan to address the findings in the report. We acknowledge management's decision on the recommendation and expect final action by March 29, 2017.

USAID produced documentation to support that it accurately reported Agency Annual Self-Inspection Program Data for FY 2015 to ISOO. After the audit fieldwork, the Office of Security gave us two missing self-inspection reports and justification for not inspecting two other offices. We adjusted the audit report to acknowledge the justifications but not the inspection reports, which we did not audit.

SCOPE AND METHODOLOGY

Scope

We conducted this performance audit in accordance with generally accepted government auditing standards. They require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, in accordance with our audit objectives. We believe that the evidence obtained provides that reasonable basis.

This is the second of two reports required by the Reducing Over-Classification Act, Public Law 111-258.

The audit objectives were to (1) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material at USAID; (2) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered at USAID; and (3) determine whether USAID addressed recommendations we made in our July 2014 report.

The audit scope covered selected USAID offices in Washington, DC (including OIG), from October 1, 2014, through June 15, 2016. We reviewed USAID's policies and procedures for its classified national security information program, including program management, security education and training, self-inspections, USAID's classification guide, fiscal year 2015 reporting to ISOO, classification markings, and implementation of prior OIG audit recommendations. At USAID missions, the Embassy's regional security officer is responsible for security programs, including handling classified information. USAID missions may not store classified information and must process classify information in the designated secured area in their respective Embassies.

To test USAID's compliance with Executive Order 13526, we reviewed 32 Code of Federal Regulations 2001, "Classified National Security Information"; USAID's ADS chapters 510 ("Mandatory Declassification Review") and 568 ("National Security Information Program"); and guidance from ISOO, such as the user guide, "Marking Classified National Security Information." We also reviewed the previous OIG report on the subject, "Evaluation of USAID's Implementation of Executive Order 13526, Classified National Security Information," Report 9-000-14-002-S, July 25, 2014.

Fieldwork was conducted at USAID's offices in Washington, DC, from June 22 to August 4, 2016.

Methodology

To answer the audit objectives, we used the Department of Defense Office of Inspector General's "A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the '"Reducing Over-Classification Act,"' as a framework for developing our audit program.

We interviewed USAID officials from the Office of Security and the Bureau for Management, as well as a sample of USOs and individuals from select bureaus and independent offices who

handle classified information. We corresponded via email with ISOO to understand the requirements for conducting Public Law 111-258 engagements. We interviewed officials from the Department of Defense, Department of State, and Millennium Challenge Corporation OIGs who were conducting Public Law 111-258 engagements on their agencies.

Our testing included the following:

- We reviewed a nonstatistical random sample of 37 out of 189 (20 percent) General Services Administration-approved security containers (safes) from the Office of Security's safe inventory. For the 37 selected safes:

  - We reviewed up to the first five classified documents that fell within the audit scope for compliance with regulatory requirements.
  - We interviewed the USO responsible for maintaining the selected safe and inspected his/her office area for compliance with regulatory requirements. The safes selected were managed by the following offices: Bureau for Asia; Executive Secretariat; Bureau for Democracy, Conflict, and Humanitarian Assistance; Bureau for Europe and Eurasia; Bureau for the Middle East; Bureau for Economic Growth, Education, and Environment; Bureau for Management; Office of Afghanistan and Pakistan Affairs; Office of Inspector General; and Office of Security.

- We reviewed a nonstatistical random sample of two out of eight (25 percent) offices that reported no safes on the Office of Security's inventory of safes: the Office of Budget and Resource Management and the Office of Human Capital and Talent Management. For these two offices, we interviewed the USOs and inspected their office areas for compliance with regulatory requirements.

- We reviewed a nonstatistical random sample of 45 out of 230 (20 percent) USAID ClassNet user accounts (derivative classification authorities) and one (out of one) original classification authority's user account as of September 30, 2015. For the 46 users selected, we reviewed the three most recent emails sent (on or before June 15, 2016) for compliance with regulatory requirements. This review included an analysis of whether documents were misclassified and the factors contributing to misclassification.

- We reviewed one originally classified document (USAID had only one) for compliance with regulatory requirements.

- We reviewed USAID's classification guide for compliance with regulatory requirements.

- We reviewed USAID's compliance with security education and training requirements, which included a review of the contents of its initial security training, 2015 annual security refresher training, original classification authority training, and the termination debriefing. Further, we verified that other specialized and required trainings, such as USO training and declassification training, existed. We also selected from our sample of 45 every fifth ClassNet user (nine users), all original classifying authorities for the audit scope (six individuals), and all derivative classifiers identified in the derivative classification document review (four) to see if the required trainings were taken and were up-to-date, and if the USOs we interviewed (12 individuals) took the USO training.

- We reviewed USAID's fiscal year 2015 Annual Senior Agency Official Self-Inspection Report and SF-311, and the Agency Security Classification Management Program Data Report submitted to ISOO for compliance with the regulatory requirements.

- We included the OIG in the sample tested, and the testing identified two exceptions: (1) OIG had not updated its performance standards to include language requiring protecting classified national security information as a required element, and (2) one document maintained in an OIG safe and six ClassNet emails did not have the correct classification markings. We will communicate the findings, along with recommendations, to the cognizant OIG office for corrective action.

Because our sample was not a statistical one, the results cannot be projected to the entire population.

To answer the audit objectives, we did not rely extensively on any of USAID's computer-processed data. However, when we tested reports generated by USAID's Learning Management System to verify and validate selected employees' test scores for the Annual Security Refresher training, we were unable to obtain the raw data of the number of questions answered correctly/incorrectly. Although we did not establish the reliability of this data, we believe that when viewed with other available evidence, they are reliable and that the opinions, conclusions, and recommendations in the report are valid.

MANAGEMENT COMMENTS

The Deputy Administrator

September 28, 2016

Mr. Thomas Yatsco
Assistant Inspector General for Audit
U.S. Agency for International Development
Washington, DC 20523

Dear Mr. Yatsco,

Thank you for the opportunity to review the draft audit report (9-000-16-001-P) on USAID's Implementation of Executive Order 13526, Classified National Security Information. I am fully committed to ensuring USAID has a world class Office of Security that is prepared to respond to the challenges that face the men and women of the Agency every day as we pursue our mission.

Upon my arrival at the Agency, I undertook a complete review of the standard operating procedures and protocols of the Office of Security. As a result of this review, new staff, policies, and procedures were put in place. In addition, as the audit notes, the Office of Security saw significant staff turnover in the past year. New staff were assigned to the Director and the Deputy Director positions in an acting capacity. Recruitment is currently underway for the Director position and will be completed within this calendar year. These interim appointments increased the professionalism of the team and reflect the need to ensure necessary expertise is present in our Office of Security staff. In addition, considerable action has already been undertaken to train staff thereby ensuring compliance with applicable policies and procedures related to security requirements.

I concur with the recommendation in the draft report and directed the Director of Security to develop and lead a comprehensive and detailed action plan focused on the findings outlined in the report. The Office of Security takes the audit findings seriously and took immediate actions to address the identified weaknesses. Accompanying this letter, please find an in-depth response from the Director of Security to the draft report.

I look forward to working with the Office of the Inspector General to continue to make progress in this area and others. Thank you for your cooperation on this matter.

Sincerely,

/s/

Alfonso E. Lenhardt
Deputy Administrator

Attachment: Response from Acting-Director of Security John Voorhees

September 28, 2016

MEMORANDUM

TO: Assistant Inspector General for Audit (AIG/A), Thomas Yatsco

FROM: Office of Security Director (Acting), John Voorhees /s/

SUBJECT: Management's Response to Draft Report on USAID's Implementation of Executive Order 13526, Classified National Security Information, (Report 9-000-16-001-P)

Thank you for your draft report on USAID's Implementation of Executive Order 13526and for the professionalism and dedication exhibited by your staff throughout this process.

Following are our comments and management decisions regarding the findings and proposed audit recommendation:

Recommendation: We recommend that the Office of the Administrator implement a corrective action plan, described in Automated Directives System (ADS) 596, to bring USAID's Classified National Security Information Program into full compliance with Executive order 13526 and Information System Oversight Office regulations and directives.

We concur with this recommendation and are currently implementing an action plan to address the findings outlined in the draft report. We plan to close out all tasks identified in the action plan within 180 days of the issuance of the final report.

Recently, the Office of Security hired a Division Chief (GS-15) to fill the senior leadership vacancy in the Counter Terrorism & Information Security Division. One of the main responsibilities of the new Division Chief is to properly oversee the implementation of the action plan under the direct supervision of the Director of Security.

Management Decisions:

1. A detailed review of ADS 568, *National Security Information Program*, is underway and will be issued after the Agency clearance process is completed. Similar reviews of other ADS chapters (ADS 101, 510, 545, 552, 562, 566, and 567) pertinent to Information Security will be conducted; recommended edits will be provided to the ADS points of contact and M/MPBP. As an example, the current Executive Order 13526 (Classified National Security Information) will be properly referenced in the aforementioned ADS chapters.

2. The two supervisors responsible for overseeing the Agency's declassification effort will initiate action to obtain Top Secret clearances.

3. The training and briefing materials for Unit Security Officers and employees will be updated based upon the findings in the draft report, to include the proper markings for derivatively classified documents and the proper utilization of the ClassNet marking tool. The professional training on these topics within the Office of Security for all Information Security Specialists has been completed.

4. The Office of Security developed and will implement a detailed plan to ensure that all Annual Security Inspections conducted in FY 2017 include proper representative samples (including classified documents in hard copy and electronic format) for classification and declassification actions conducted within the Bureaus and Independent Offices (B/IO).

5. A formal written designation was made for the Unit Security Officer in the Office of the Executive Secretariat that serves the Office of Budget and Resource Management.

6. The Director of Security designated an individual outside the Information and Industrial Security Branch to serve as the Office's Unit Security Officer. In addition, all information security inspections conducted for the Office of Security in FY 2017 will be performed with a Unit Security Officer from another B/IO to ensure an impartial inspection.

7. The Office of Security initiated a complete physical inventory of all classified safes in order to confirm the accuracy of the current on-hand inventory.

8. The Agency Classification Guide was updated on September 13, 2016, to include a point of contact and will be distributed to all Agency ClassNet users.

9. The SF-311 (Agency Security Classification Management Program Data) for FY 2016 will be completed in accordance with written guidelines developed by the Information Security Oversight Office (ISOO).

10. The 11 recommendations outlined in the 2014 OIG audit report related to USAID's compliance with Executive Order 13526 have been reviewed and incorporated into the action plan to ensure consistent and effective implementation.

I ask that you reconsider the characterization of the Agency as having a lax security culture that is pervasive. I do not believe this characterization is accurate. I have found the Agency's leaders and employees very willing to take the necessary and appropriate actions when dealing with both classified and unclassified information. This comes from my direct involvement with information during sensitive briefings and the Agency-wide handling and management of both hard copy and electronic documents. Since developing the action plan, I am confident that its implementation will be strongly supported within the Agency.

Subsequent to the final audit out brief, the Office of Security was able to produce documentation to support that the FY 2015 Agency Annual Self Inspection Program Data Report to the Information Security Oversight Office was accurate in terms of the number of Bureau and Independent Offices that were inspected. We ask that this be reflected in the final report.

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
https://oig.usaid.gov/
Audit Task No. 99100616