OFFICE OF INSPECTOR GENERAL

AUDIT OF USAID'S FEDERAL INFORMATION SECURITY MANAGEMENT ACT ACTION PLAN

AUDIT REPORT NO. A-000-16-004-P
DECEMBER 22, 2015

WASHINGTON, D.C.

Office of Inspector General

December 22, 2015

MEMORANDUM

TO: Chief Information Officer, Jay Mahanand

FROM: Deputy Assistant Inspector General, IG/A/ITA, Alvin Brown /s/

SUBJECT: Audit of USAID's Federal Information Security Management Act Action Plan (Report No. A-000-16-004-P)

This memorandum transmits the final report prepared by CliftonLarsonAllen LLP on the subject audit. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (Clifton) to conduct the audit.

According to Clifton, it followed *Government Auditing Standards* issued by the U.S. Comptroller General in conducting the audit. The objective was to determine what progress USAID has made in implementing its Federal Information Security Management Act (FISMA) action plan. To answer that, Clifton reviewed documents supporting the action plan, conducted interviews with USAID personnel, and reviewed legal and regulatory requirements stipulated in FISMA. Fieldwork was conducted at USAID offices in Washington, D.C., and Arlington, Virginia, from August 6 to October 23, 2015. Clifton is responsible for the enclosed auditor's report and the conclusions expressed in it.

In carrying out its oversight responsibilities, OIG reviewed the report and related audit documentation to determine whether Clifton complied with U.S. generally accepted government auditing standards. Our review was different from an audit in accordance with those standards and was not intended to enable us to express, and we do not express, an opinion on USAID's FISMA action plan. Our review did not disclose any instances in which Clifton did not comply, in all material respects, with applicable standards.

The audit concluded that USAID has made progress in implementing its action plan. However, the process for tracking and fully implementing corrective actions needs improvement. The Agency needs to:

- Make sure corrective actions are completed by target completion dates.
- Make sure that the activities/findings submitted for closure have been fully and effectively implemented.

Recommendations addressing the findings were noted in the past year's FISMA action plan audit. However, the procedures were not fully implemented, and USAID had not closed the recommendations. This report does not make any new recommendations.

Management comments were not required since the report makes no recommendations. Nevertheless, we gave the Agency an opportunity to provide comments on the report as a whole, and the Agency had no comments.

OIG appreciates the cooperation and courtesies extended to our staff and to the staff of Clifton.

Audit of USAID's Federal Information Security Management Act of 2002, as amended, Corrective Action Plan

Fiscal Year 2015

Final Report

4250 N. Fairfax Drive
Suite 1020
Arlington, Virginia 22203
tel: 571-227-9500
fax: 571-227-9552

www.claconnect.com

TABLE OF CONTENTS

SUMMARY OF RESULTS

Background

The Federal Information Security Management Act of 2002[1] (FISMA), as amended[2] requires agencies to develop, document, and implement an agencywide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. Because the U.S. Agency for International Development (USAID) is a federal agency, it is required to comply with federal information security requirements.

The Office of the Inspector General's fiscal year 2012 independent FISMA audit[3] noted that USAID had developed and documented the majority of their information security policies and procedures required under FISMA; however, based on the results of the audit and follow-up on the status of issues identified in prior-year audits, it was determined that management's implementation of these policies and procedures is not effective. The audit report identified a number of information system weaknesses that, if exploited, could adversely impact the confidentiality, integrity, and availability of USAID's data and information systems and could ultimately have a negative impact on the agency's ability to protect the security of its information or information systems. The fiscal year 2012 FISMA report resulted in a significant deficiency for FISMA compliance, a low rate of overall compliance, and a material weakness in the Agency's 2012 Financial Report.

In response, USAID's Bureau for Management's Office of the Chief Information Officer (M/CIO) developed a three-year corrective action plan (CAP) dated April 16, 2013, with the goal of obtaining a top FISMA score. The plan was divided into three phases and consisted of seven critical categories of activities that relate to the OIG findings, including governance, centralized IT, systems development, critical security controls, identity and access management, performance monitoring, and additional FISMA audit activities. Within these seven categories, there were 48 activities ranging from centralizing IT procurement to the removal of unauthorized systems over time.

During fiscal year 2015, M/CIO updated its approach to address the CAP and updated an action plan with the goal of improving the security of USAID IT assets and improving the Agency's FISMA score. The updated actions address specific open audit findings that either directly or indirectly relate to the original CAP, including: improved governance; centralized review/approval of Agency IT; improved systems development lifecycle (SDLC) methodology; implementing specific critical security controls to include identity and access management (PIV/HSPD-12); and iterative stages of Department of

[1] Enacted as Title III of the E-Government Act of 2002, Public Law 107-347 (2002). Section 301 of the Act added a new subchapter on information security to the United States Code at 44 U.S.C 3541-3549.

[2] The Federal Information Security Modernization Act of 2014 - amends the FISMA Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

[3] *Audit of USAID's Fiscal Year 2012 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-000-13-003-P, November 14, 2012).

Homeland Security Continuous and Diagnostic Monitoring (CDM). Within each activity, M/CIO has identified specific milestones, with anticipated completion dates, to measure plan progress.

The original CAP dated April 16, 2013, was designed to address root cause issues for the significant deficiency rather than specific audit findings. The approach was designed to prevent future findings and address strategic-level issues that were not necessarily system specific. Although there was an initial mapping of CAP activities to open audit findings, there was not a direct correlation for each finding. Therefore, while M/CIO prepared to address longer-term projects and other issues, there was no significant progress being made to address immediate actions required to close the prior year's audit findings. As a result, M/CIO has updated the original CAP to specifically focus on the open audit findings from the fiscal year 2012 FISMA audit report.

Audit Objective

The USAID Office of Inspector General engaged CliftonLarsonAllen LLP (CLA) to conduct an audit to assess the progress of USAID in implementing the FISMA CAP. The objective of this performance audit was to determine what progress USAID has made in implementing its FISMA CAP. The audit also included procedures to determine the status of the four prior year recommendations made to USAID in the prior year audit of USAID's FISMA Action Plan.[4]

Our audit was performed 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Results

The audit concluded that USAID has made progress in implementing corrective actions; however, the process for tracking and fully implementing corrective actions needs improvement. Specifically, USAID needs to:

- Ensure corrective actions are completed by target completion dates.
- Ensure that the activities/findings submitted for closure have been fully and effectively implemented.

Recommendations addressing the findings were noted in the prior year FISMA Action Plan audit;[5] however, procedures were not fully implemented and USAID had not closed the recommendations. As a result, the report does not make any new recommendations. The details of the findings are discussed in the following section.

Detailed findings appear in the following section. Appendix I describes the audit scope and methodology.

[4] *Audit of USAID's Federal Information Security Management Act of 2002 Action Plan* (Audit Report No. A-000-15-004-P, November 5, 2014).

[5] Recommendations 2, 3, and 4, *Audit of USAID's Federal Information Security Management Act of 2002 Action Plan* (Audit Report No. A-000-15-004-P, November 5, 2014).

AUDIT FINDINGS

USAID's Process for Tracking and Implementing Its FISMA Corrective Action Plan Needs Improvement

To address the issues noted in the fiscal year 2012 FISMA Audit[6] and recommendations made in the prior year audit of USAID's FISMA Action Plan,[7] USAID's Bureau for Management's Office of the Chief Information Officer (M/CIO) updated the FISMA Corrective Action Plan (CAP) and associated activities to address past years' open FISMA audit findings. The updated actions address specific open audit findings that either directly or indirectly aligns activities documented in the original CAP dated April 16, 2013. As a result, M/CIO has updated the original CAP to specifically focus on the open audit findings from the prior FISMA audits. In addition, M/CIO has approved and implemented a project charter to manage, track and report on the activities associated with the updated FISMA CAP. Due to M/CIO's updated approach to the CAP, our audit focused on a review of the CAP Activities/FISMA Tracker.

USAID has made progress in implementing corrective actions; however, the process for tracking and fully implementing corrective actions needs improvement. Specifically, we noted:

- Based on a review of the CAP Activities/FISMA Finding Tracker as of October 6, 2015, we noted three out of 21 findings/activities remain open. Two of the three open activities had target completion dates that were past due. Upon notification to management, the past due items were updated with new target completion dates. USAID management noted that the original due dates were based on the CIO's requirement to close all past due audit recommendations by the end of fiscal year 2015, to the extent that it was feasible. However, due to the complexity of some of the audit recommendations, combined with various external dependencies several of the recommendations could not be closed by end of fiscal year 2015. M/CIO' new target date is December 31, 2015, at which time USAID will re-evaluate items that remain open to make recommendations and establish new milestones and timelines.

  Since management has taken corrective action to update the overdue items with new estimated completion dates, we will not make a recommendation addressing this issue.

- We noted that 18 out of 21 findings/activities were submitted for closure to the Office of the Chief Financial Officer (OCFO's) Audit, Performance, & Compliance Division (APC) for review and approval. However, two of the 18 findings/activities submitted for closure to APC were rejected and one of the items was rejected twice for inadequate support to close the finding.

[6] *Audit of USAID's Fiscal Year 2012 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-000-13-003-P, November 14, 2012).
[7] *Audit of USAID's Federal Information Security Management Act of 2002 Action Plan* (Audit Report No. A-000-15-004-P, November 5, 2014).

- We noted one activity was submitted for closure to APC; however, the recommendation has not been fully implemented. Specifically, USAID submitted for closure finding related to transitioning all applicable applications and information systems to National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. However, as reported in the fiscal year 2015 FISMA audit, the recommendation remains open.[8]

  The above items occurred because management did not ensure that the activities had been fully and effectively implemented before submitting them for closure to APC.

Even though USAID has made some progress implementing corrective actions and closing prior year FISMA audit findings, the fiscal year 2015 FISMA audit[9] still noted a significant deficiency in USAID's information security program. The significant deficiency remained for fiscal year 2015 since the audit continued to identify a lack of an effective risk management program and continued open FISMA-related audit recommendations from prior years'. The audit noted that USAID has not fully addressed recommendations made in prior year FISMA audits. In addition, the audit identified an additional 17 new recommendations to assist USAID in strengthening its information security program and bring it to compliance with FISMA, OMB, and NIST requirements. Therefore, the current approach to addressing FISMA-related weaknesses does not seem to be addressing the underlying weaknesses in USAID's information security program.

NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Task 3.4 RMF Step 4 – Assess Security Controls, Supplemental Guidance, states:

> Conducting security control assessments in parallel with the development/acquisition and implementation phases of the life cycle permits the identification of weaknesses and deficiencies early and provides the most cost-effective method for initiating corrective actions. Issues found during these assessments can be referred to authorizing officials for early resolution, as appropriate. The results of security control assessments carried out during system development and implementation can also be used (consistent with reuse criteria) during the security authorization process to avoid system fielding delays or costly repetition of assessments.

In addition, Task 4-3: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment, Supplemental Guidance, states:

> The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the *security assessment report*. The security assessment report is one of three key documents in the security authorization package developed for authorizing

[8] Finding 12, *Audit of USAID's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, As Amended* (Audit Report No. A-000-15-010-P, September 25, 2015).
[9] *Audit of USAID's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, As Amended* (Audit Report No. A-000-15-010-P, September 25, 2015).

officials. The assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the assessor's findings. The security assessment report is an important factor in an authorizing official's determination of risk to organizational operations and assets, individuals, other organizations, and the Nation. Security control assessment results are documented at a level of detail appropriate for the assessment in accordance with the reporting format prescribed by organizational and/or federal policies. The reporting format is also appropriate for the type of security control assessment conducted (e.g., developmental testing and evaluation, self-assessments, independent verification and validation, independent assessments supporting the security authorization process or subsequent reauthorizations, assessments during continuous monitoring, assessments subsequent to remediation actions, independent audits/evaluations).

Without an effective and consistent corrective action process for addressing and monitoring known weaknesses, management cannot ensure their implemented activities are effectively improving their information security program in support of FISMA. In addition, without sufficient documentation to justify closure of findings, USAID cannot ensure that corresponding security risks have been fully mitigated.

Recommendations addressing these findings were noted in the prior year FISMA Action Plan audit;[10] however, procedures were not fully implemented and USAID had not closed the recommendations. Therefore, we have not made additional recommendations to address these weaknesses.

[10] Recommendations 2, 3, and 4, *Audit of USAID's Federal Information Security Management Act of 2002 Action Plan* (Audit Report No. A-000-15-004-P, November 5, 2014).

SCOPE AND METHODOLOGY

Scope

We conducted this audit in accordance with generally accepted Government auditing standards, as specified in the Government Accountability Office's 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The audit was designed to determine what progress USAID has made in implementing its FISMA Corrective Action Plan (CAP). The audit also included procedures to determine the status of the four prior year recommendations made to USAID in the prior year audit of USAID's FISMA Action Plan.[11]

The audit fieldwork was performed at the USAID offices in Washington, D.C. and Arlington, VA from August 6, 2015, to October 23, 2015.

Methodology

To assess USAID's progress in implementing the FISMA CAP, we conducted interviews with USAID personnel and reviewed legal and regulatory requirements stipulated in FISMA. We also reviewed documents supporting USAID's FISMA CAP. These documents included, but were not limited to, USAID's (1) 2015 Corrective Action Plan; (2) CAP Project Charter; and (3) CAP Activities/FISMA Finding Tracker. In addition, where findings/ activities were identified as completed, we conducted additional interviews and reviewed supporting documentation to evaluate management's implementation.

In testing for the adequacy and effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk, and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review. In some cases, this resulted in selecting the entire population. However, in cases that we did not select the entire audit population, the results cannot be projected and if projected may be misleading.

[11] *Audit of USAID's Federal Information Security Management Act of 2002 Action Plan* (Audit Report No. A-000-15-004-P, November 5, 2014).

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/
Audit Task No. AA101215