OFFICE OF INSPECTOR GENERAL

USAID HAS IMPLEMENTED CONTROLS IN SUPPORT OF FISMA, BUT IMPROVEMENTS ARE NEEDED

AUDIT REPORT NO. A-000-17-001-C
OCTOBER 27, 2016

WASHINGTON, DC

Office of Inspector General

October 27, 2016

MEMORANDUM

TO: Deputy Administrator, Ambassador Alfonso E. Lenhardt
Chief Information Officer, Jay Mahanand
Chief Financial Officer, Reginald Mitchell
Chief Human Capital Officer, Kimberly Lewis
Director, Office of Management Policy, Budget, and Performance, Colleen Allen

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

SUBJECT: USAID Has Implemented Controls in Support of FISMA, but Improvements Are Needed (A-000-17-001-C)

This memorandum transmits our final report on the subject audit. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (Clifton) to conduct the audit. According to Clifton officials, this audit was performed in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

In carrying out our oversight responsibilities, we 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, nor do we express, an opinion on USAID's compliance with the Federal Information Security Modernization Act of 2014 (FISMA). Clifton is responsible for the enclosed auditor's report and its conclusions. We did not find any instances of Clifton not complying, in all material respects, with applicable standards.

The audit objective was to determine whether USAID implemented certain security controls for selected information systems in support of FISMA. (Appendix IV lists controls and systems selected, and rates their effectiveness.) To answer the audit objective, Clifton tested USAID's implementation of selected controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." The audit included five systems:

- Agency for International Development Network
- Phoenix Financial System
- Global Acquisition and Assistance System
- WebTA
- Enterprise Loan Management System

Clifton conducted fieldwork at USAID's headquarters in Washington, DC, from March 31 through September 12, 2016.

The audit concluded that USAID generally complied with FISMA requirements by implementing 126 of 144 selected security controls for the 5 information systems. However, USAID did not implement 18 controls designed to preserve the confidentiality, integrity, and availability of its information and information systems.

USAID complied with many FISMA requirements, including the following:

- Maintaining an effective security awareness training program for employees.
- Implementing an effective configuration management program.
- Implementing an effective program for incident handling and response.
- Implementing an effective system acquisition and services program.
- Implementing an effective identification and authentication program.
- Implementing an effective contingency planning program.

However, USAID still needs to do the following:

- Strengthen the structure of the Office of the Chief Information Officer.
- Separate the deputy chief information officer's and the chief information security officer's responsibilities and duties.
- Strengthen security controls for patch and configuration management.
- Maintain current system authorizations to operate and assess system risks.
- Strengthen webTA privacy controls to minimize exposure of personally identifiable information.
- Strengthen webTA account management controls.
- Strengthen the plan of action and milestones process.
- Strengthen personnel out-processing procedures.
- Improve physical access controls for information technology rooms.
- Maintain current information system agreements.
- Strengthen monitoring of third-party system providers.
- Strengthen monitoring of the Phoenix application.
- Implement controls for role-based training.

To address the weaknesses identified in Clifton's report, OIG makes the following recommendations to USAID management.

> ***Recommendation 1.*** *We recommend that the Deputy Administrator develop and implement a plan to ensure the chief information officer position reports directly to the Administrator or Deputy Administrator as required by the Federal Information Technology Acquisition Reform Act of 2014 and the Clinger-Cohen Act of 1996.*
>
> ***Recommendation 2.*** *We recommend that the Deputy Administrator develop a written plan to ensure the chief information officer has a significant role in the management, governance, and oversight of information technology as required by the Federal Information Technology Acquisition Reform Act of 2014.*

Recommendation 3. *We recommend that the chief information officer implement a plan to segregate the deputy chief information officer and chief information security officer positions and appoint in writing a senior-level chief information security officer in accordance with the Federal Information Security Modernization Act.*

Recommendation 4. *We recommend that the chief information officer remediate vulnerabilities on the network identified by the Office of Inspector General's contractor, as appropriate, or document acceptance of the risks of those vulnerabilities.*

Recommendation 5. *We recommend that the chief information officer document and implement a process to track and remediate persistent vulnerabilities promptly, or document acceptance of the risk of those vulnerabilities.*

Recommendation 6. *We recommend that the chief information officer document and implement a process to ensure vulnerability assessment tools are configured to detect vulnerabilities previously not detected by internal scans*.

Recommendation 7. *We recommend that the chief information officer document and implement a process to centrally manage printers and apply hardened security configurations prior to placing printers into the production environment.*

Recommendation 8. *We recommend that the chief information officer document and implement a plan to make sure all internal and external systems have a current authority to operate.*

Recommendation 9. *We recommend that the chief information officer, in coordination with the chief financial officer, document and implement a procedure to minimize exposure of personally identifiable information in webTA.*

Recommendation 10. *We recommend that the chief information officer, in coordination with the chief financial officer, document and implement a procedure to complete, approve, and maintain access request forms for webTA users in accordance with policies, or document acceptance of the risk of not having such controls.*

Recommendation 11. *We recommend that the chief information officer, in coordination with the chief financial officer, document and implement a procedure to review webTA accounts periodically for appropriateness in accordance with policies or document acceptance of the risk of not having such controls.*

Recommendation 12. *We recommend that the chief information officer develop and implement a written process to validate that the AIDnet plan of action and milestones is completed and updated promptly.*

Recommendation 13. *We recommend that the director of the Office of Management Policy, Budget, and Performance, in coordination with the chief information officer and the chief human capital officer, document and implement a procedure to promptly remove system accounts associated with people no longer at the Agency.*

Recommendation 14. *We recommend that the chief information officer, in coordination with the chief human capital officer, document and implement a process to verify that all employees' exit clearance forms are completed and maintained in accordance with policy.*

Recommendation 15. *We recommend that the chief information officer document and implement a procedure to complete, approve, and maintain access request forms for individuals requiring access to the information technology rooms in the Ronald Reagan Building and Two Potomac Yard locations.*

Recommendation 16. *We recommend that the chief information officer document and implement a procedure to review individual access periodically and ensure only authorized personnel have access to information technology rooms in the Ronald Reagan Building and Two Potomac Yard locations.*

Recommendation 17. *We recommend that the chief information officer document and implement a validation process to confirm that all memorandums of understanding and interconnection security agreements are current and approved.*

Recommendation 18. *We recommend that the chief financial officer document and implement a procedure to review third-party assessment reports to ensure complementary user entity controls have been implemented for the Enterprise Loan Management System.*

Recommendation 19. *We recommend that the chief financial officer document and implement a procedure to review active Enterprise Loan Management System accounts that have not been used for a specified period and disable them as necessary in accordance with agency policy.*

Recommendation 20. *We recommend that the chief financial officer document and implement a procedure to periodically review the Department of State vulnerability scan results and remediation actions supporting the Phoenix application.*

In finalizing the report, Clifton evaluated USAID's responses on the 20 recommendations. Based on those responses, we acknowledge management decisions on recommendations 1 through 20, though we disagree with the decisions on recommendations 1, 3, and 15. In addition, we acknowledge management's decision on recommendation 6 but disagree that final action has been taken. Further, we acknowledge final action on recommendations 2, 12, and 14.

Please provide evidence of final action on the open recommendations to the Audit Performance and Compliance Division.

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

The United States Agency for International Development (USAID) Has Implemented Many Controls in Support of FISMA, But Improvements Are Needed

Fiscal Year 2016

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

The Federal Information Security Modernization Act of 2014[1] (FISMA), requires agencies to develop, document, and implement an agency wide 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 act also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget and Congressional committees on the effectiveness of their information security program. In addition, FISMA has established that the standards and guidelines issued by the National Institute of Standards and Technology (NIST) are mandatory for Federal agencies.

The USAID Office of Inspector General engaged CliftonLarsonAllen LLP to conduct an audit in support of the FISMA requirement for an annual evaluation of USAID's information security program. The objective of this performance audit was to determine whether USAID implemented selected security controls for selected information systems[2] in support of FISMA.

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.

For this audit, we reviewed the following five systems:

- Agency for International Development Network (AIDNet)
- Phoenix Financial System (Phoenix)
- Global Acquisition and Assistance System (GLAAS)
- WebTA (Web-based Time & Attendance)
- Enterprise Loan Management System (ELMS)

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management 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 the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] See Appendix IV for a list of systems and controls selected.

Results

The audit concluded that USAID generally complied with FISMA requirements by implementing 126 of 144 selected controls[3] for selected information systems. Although we found some controls that need improvement, USAID complied with following requirements:

- Maintaining an effective security awareness training program for its employees.
- Implementing an effective configuration management program.
- Implementing an effective incident handling and response program.
- Implementing an effective system service and acquisition program.
- Implementing an effective identification and authentication program.
- Implementing an effective contingency planning program.

Although USAID generally had policies and procedures for its information security program, its implementation of those policies for 18 of the 144 selected controls was not fully effective to preserve the confidentiality, integrity, and availability of USAID's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified several areas in USAID's information security program that needed to be improved. Specifically, USAID needs to:

- Strengthen the organizational structure for the Office of the Chief Information Officer.
- Separate the Deputy Chief Information Officer and Chief Information Security Officer's responsibilities and duties.
- Strengthen security controls surrounding patch and configuration management.
- Maintain current system authorizations to operate and assess system risks.
- Strengthen WebTA privacy controls to minimize personally identifiable information.
- Strengthen WebTA account management controls.
- Strengthen the plan of action and milestones process.
- Strengthen personnel out-processing procedures.
- Improve physical access controls for information technology rooms.
- Maintain current information system agreements.

[3] See Appendix IV – Summary of Results of Each Control Reviewed.

- Strengthen the monitoring of the third party providers.

- Strengthen the monitoring of the Phoenix Application.

- Implement controls surrounding role-based training.

Consequently, USAID's operations and assets are at risk of unauthorized access, misuse and disruption. We made 20 recommendations to assist USAID in strengthening its information security program. (See pages 4 – 19)

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

In response to the draft report, USAID outlined and described its plans to address all 20 audit recommendations. Based on our evaluation of management comments, we acknowledge management decisions on recommendations 1 through 20, though we disagree with the decisions for recommendations 1, 3 and 15 and respectfully request USAID to revise them. In addition, we acknowledge management's decision on recommendation 6; but we disagree that final action has been taken. Further, we acknowledge final action has been taken on recommendations 2, 12 and 14. USAID's comments are included in their entirety in Appendix II.

AUDIT FINDINGS

1. USAID Needs to Strengthen the Organizational Structure for the Office of the Chief Information Officer

As required by the Clinger-Cohen Act of 1996, Public Law 104-106 - Feb. 10, 1996 and as left in place by the Federal Information Technology Acquisition Reform Act (FITARA), Public Law 113-291, Dec. 19, 2014, "the CIO shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter." Furthermore, FITARA states, "The head of each covered agency shall ensure that the Chief Information Officer of the agency has a significant role in-(i) the decision processes for all annual and multiyear planning, programming budgeting, and execution decisions and (ii) the management, governance, and oversight processes related to Information Technology (IT).

The USAID Chief Information Officer (CIO) position did not report directly to the agency Administrator or Deputy Administrator as required by FITARA and the Clinger-Cohen Act of 1996. Instead, the USAID CIO reported directly to the Assistant Administrator for the Bureau of Management. As a result, the CIO may have limited power in ensuring IT issues and projects are funded and provided a priority level commensurate with the direction and goals of the Agency as a whole. As noted in Finding 4, the CIO did not have full authority in ensuring systems not owned by the CIO office were fully funded and prioritized to ensure they timely received a proper Authority to Operate (ATO). Findings 5, 6, 11, and 12 also identify weaknesses in systems not owned by the CIO office. By not having full authority over these systems, CIO faces challenges in ensuring all USAID systems are properly secured, operating with valid ATOs and that only authorized systems are operating within the environment.

USAID management indicated that the issue of the CIO's reporting relationship with the Administrator or Deputy Administrator remains in a pending status until a discussion can be had with senior leadership.

By not ensuring that the CIO position reports directly to the USAID Administrator or Deputy Administrator, the CIO faces challenges in fully exercising duties and responsibilities of implementing an effective and efficient information technology program for the agency. As a result, we recommend the following:

> ***Recommendation 1:*** *We recommend that the Deputy Administrator develop and implement a plan to ensure the chief information officer position reports directly to the Administrator or Deputy Administrator as required by the Federal Information Technology Acquisition Reform Act of 2014 and the Clinger-Cohen Act of 1996.*
>
> ***Recommendation 2:*** *We recommend that the Deputy Administrator develop a written plan to ensure the chief information officer has a significant role in the management, governance, and oversight of information technology as required by the Federal Information Technology Acquisition Reform Act of 2014.*

2. Deputy Chief Information Officer and Chief Information Security Officer Need Formal Separation of Responsibilities and Duties

The FISMA Act of 2014, states the following regarding federal agency responsibilities:

> **§ 3554. Federal agency responsibilities**
> (a) IN GENERAL.—The head of each agency shall—
> (A) designate a senior agency information security officer who shall—
> * * *
> (iii) have information security duties as that official's primary duty; and
> (iv) head an office with the mission and resources to assist in ensuring agency compliance with this section.

In addition, USAID Automated Directive System (ADS) Chapter 545, *Information Systems Security,* dated March 9, 2016, Section 545.2, *Primary Responsibility,* states the following:

> The Agency's senior information security official is the Chief Information Security Officer (CISO). The CISO's duties include: (i) carrying out the CIO security responsibilities under the Federal Information Security Management Act; and (ii) serving as the primary liaison for the CIO to the organization's Authorizing Officials, information System Owner, common control providers, and Information System Security Officers.

We found that appropriate segregation of duties was not maintained because USAID combined the roles of the Deputy CIO and the Chief Information Security Officer (CISO) to one individual. As a result, that individual performs security control activities and at the same time reviews that activity for compliance with FISMA. Previously, USAID had a CISO performing information security duties as their official primary duty. However, during fiscal year 2016, USAID designated both the Deputy CIO and CISO to one individual and had structured the Deputy CIO role to functions that focus heavily on cybersecurity with secondary duties to include IT Operations.

With the CISO's responsibilities not being independent from the IT operation's function, the ability to independently and effectively assess compliance with security requirements may diminish.

> ***Recommendation 3:*** *We recommend that the chief information officer implement a plan to segregate the deputy chief information officer and chief information security officer positions and appoint in writing a senior-level chief information security officer in accordance with the Federal Information Security Modernization Act.*

3. USAID Needs to Strengthen Security Controls Surrounding Patch and Configuration Management

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and*

Organizations, security control security control SI-2 states the following regarding flaw remediation:

> The organization:
> * * *
> c. Installs security-relevant software and firmware updates within [*Assignment: organization defined time period*] of the release of the updates.

In addition, security control RA-5, states the agency is responsible for the following:

> The organization:
> * * *
> d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk.

Independent scans of USAID's networks at the Ronald Reagan Building, Two Potomac Yard, Office of Foreign Disaster Assistance, and sample of missions (Georgia, El Salvador, Thailand, and Ghana) identified critical and high risk vulnerabilities related to patch management, configuration management, and unsupported software. Of the vulnerabilities identified, 495 unique vulnerabilities were publically known prior to 2016.

USAID indicated that historically they did not have adequate tools to provide visibility to monitor the network. For example, USAID noted that during the Department of Homeland Security penetration test in March of 2016, they did not detect the activities of the testers. As a result, USAID had been working to increase their monitoring capabilities including the implementation of a network intrusion protection system. However, USAID did identify several of our Nessus scans during the vulnerability assessment phase.

Management indicated that they also faced several logistic issues in updating remote laptops for traveling personnel. Laptop owners may not have their laptops on the network long enough to receive all updates. Some owners may also have corrupted Microsoft System Center Configuration Manager client's software which would prevent the laptop from receiving updates. In addition, remote end users did not have the capability to download patches through a virtual private network.

In addition, patch management is a distributed responsibility with local missions and site management receiving monthly vulnerability grades. However, the focus on grades may not prevent persistent vulnerabilities from existing from month to month especially if vulnerabilities were not identified by vulnerability scans. For example, a comparison of our independent scans, which were performed with the vulnerability assessment tool Nessus, and USAID's IP360 scans from the same time period identified several configuration vulnerabilities that were not found in USAID's scans including Microsoft Unquoted Service Path Enumeration and Insecure Windows Service Permissions. The difference in scans may be due to the configuration variances or the difference in vulnerability signatures for the scanning tools. These variances were observed in two instances where USAID did not have enough IP360 licenses to be able to scan all hosts currently identified for scanning and vulnerability signatures were being excluded from reporting.

Furthermore, information technology assets such as printers were not centrally managed or hardened prior to being placed into the production environment.

Unmitigated vulnerabilities on the USAID network can compromise the confidentiality, integrity, and availability of information on the network. For example:

- An attacker may leverage known vulnerabilities to execute arbitrary code.
- USAID employees may be unable to access systems.
- USAID data may be lost, stolen or compromised.

> ***Recommendation 4:*** *We recommend that the chief information officer remediate vulnerabilities on the network identified by the Office of Inspector General's contractor, as appropriate, or document acceptance of the risks of those vulnerabilities.*
>
> ***Recommendation 5:*** *We recommend that the chief information officer document and implement a process to track and remediate persistent vulnerabilities promptly, or document acceptance of the risk of those vulnerabilities.*
>
> ***Recommendation 6:*** *We recommend that the chief information officer document and implement a process to ensure vulnerability assessment tools are configured to detect vulnerabilities previously not detected by internal scans*.
>
> ***Recommendation 7:*** *We recommend that the chief information officer document and implement a process to centrally manage printers and apply hardened security configurations prior to placing printers into the production environment.*

4. USAID Needs to Maintain Current System Authorizations to Operate and Assess System Risks

NIST Special Publication 800-53, Revision 4, security control CA-2, states the following regarding security assessment:

> The organization:
>
> * * *
>
> b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
> c. Produces a security assessment report that documents the results of the assessment; and
> d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].

In addition, security control CA-6, states the following regarding security authorization:

> The organization:
>
> * * *

c. Updates the security authorization [*Assignment: organization-defined frequency*].

Furthermore, security control RA-3, states the following regarding risk assessment:

The organization:

* * *

e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

The Authority to Operate (ATO) had expired for several internal and external systems. Specifically, 5 of 25 internal USAID systems and 7 of 25 external systems had expired ATOs. Management indicated that the systems were either in process of completing their re-authorization, waiting on funding to do the re-authorization, awaiting decommissioning of the system, or looking for an outside vendor to assist with the assessment process.

In addition, USAID did not properly assess system risks on AIDNet and WebTA. Specifically, we noted:

- WebTA security assessment and authorization (SA&A) documentation including the System Security Plan, Risk Assessment, Security Assessment Report and Plan of Action and Milestones were outdated. In addition, the current System Security Plan did not fully address NIST SP 800-53, Revision 4, privacy controls. The last SA&A of the system was completed in 2013; however, continuous monitoring activities had not occurred for the system to include maintaining up-to-date security documentation. In addition, the WebTA ATO expired on July 22, 2016. In fiscal year 2016, USAID began the process for re-authorizing the system prior to expiration of the ATO; however, management encountered delays due to a server security patch that was outside the purview of the WebTA support team. An ATO extension had been granted for six months to complete the SA&A process.

- The annual security controls assessment and an annual update to the risk assessment had not been completed for the AIDNet system. Management indicated that as part of continuous monitoring, one-third of controls are assessed on an annual basis and all controls are assessed at least once every three years as part of the triennial SA&A process. However, management did not provide evidence of a completed security assessment or an updated risk assessment for fiscal years 2015 and 2016. The last security controls assessment and risk assessment were completed in 2014. Management indicated that during 2015, an assessment was not completed as the focus of testing was around the controls that failed during the 2014 assessment, causing the system to get a 1 year temporary ATO. The failed controls were tested in fiscal year 2015 and the system was granted a full ATO. However, the risk assessment was not updated in 2015. The 2016 annual control testing was on-going and was expected to be completed by the end of the fiscal year.

By not completing continuous monitoring activities and assessing system risk, there is an increased risk that the Authorizing Official does not have the appropriate knowledge to ensure mitigation of known risks and make risk-based decision on whether to authorize the system to continue to operate. In addition, there is an increased risk that USAID systems are susceptible to risks of unauthorized access, viruses, malicious code, and exploitable vulnerabilities.

A recommendation addressing the weaknesses related to continuous monitoring activities was made in the fiscal year 2015 audit;[4] however, procedures were not fully implemented and USAID had not closed the recommendation. Therefore, we are not making additional recommendations at this time. However, we recommend the following for the remaining weaknesses:

> ***Recommendation 8:*** *We recommend that the chief information officer document and implement a plan to make sure all internal and external systems have a current authority to operate.*

5. WebTA Privacy Controls Need Strengthening

NIST Special Publication 800-53, Revision 4, privacy control DM-1, states the following regarding minimization of personally identifiable information:

> The organization:
> a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
> b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
> c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

In addition, privacy control DM-3, states the following regarding minimization of personally identifiable information used in testing, training, and research:

> The organization:
> a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and
> b. Implements controls to protect PII used for testing, training, and research.

Controls were not adequate to ensure minimization of personally identifiable information within the WebTA application. Specifically, an employee's full social security number was viewable to a number of roles within WebTA. Management was in discussions with the vendor to restrict displaying of full social security numbers within the application and

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

to only allow only human resource administrators and system administrators to view full social security numbers. However, the controls had not been implemented at the time of the audit.

By not ensuring minimization of personally identifiable information, there is an increased risk of unauthorized disclosure or misuse of the information. As a result, we recommend the following:

> ***Recommendation 9:*** *We recommend that the chief information officer, in coordination with the chief financial officer, document and implement a procedure to minimize exposure of personally identifiable information in webTA.*

6. WebTA Account Management Controls Need to be Strengthened

NIST Special Publication 800-53, Revision 4, security control AC-2, states the following regarding account management:

> The organization manages information system accounts, including:
>
> * * *
>
> e. Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts.
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].
> g. Monitors the use of information system accounts.
> h. Notifies account managers:
>
> 1. When accounts are no longer required;
> 2. When users are terminated or transferred; and
> 3. When individual information system usage or need-to-know changes.
>
> i. Authorizes access to the information system based on:
>
> 1. A valid access authorization;
> 2. Intended system usage; and
> 3. Other attributes as required by the organization or associated missions/business functions.
>
> j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*].

In addition, USAID ADS Chapter 545, Section 545.3.5.2, *Access Control,* states "(3) (SOs) [system owner] must document and implement access control policy and procedures to protect resources from unauthorized alteration, loss, unavailability, or disclosure."

Furthermore, Section 545.3.5.3, *b. Automatic Session Termination*, states "(3) (SOs) [system owner] must configure networked applications or systems to automatically lock any user session in accordance with the appropriate CIO-approved configuration guide. Without guidance, the session must lock following twenty (20) minutes of inactivity."

Controls were not adequate to ensure USAID effectively managed WebTA accounts. Specifically, we noted the following regarding WebTA account management controls:

- User access forms were not in place for granting access to the WebTA application as required by policy. Specifically, of the 600 active WebTA users, 25 of a sample of 25 users did not have approved access request forms on file. Management indicated that access request forms were not used because access for the application was granted upon obtaining an AIDNet user account.

- USAID did not recertify WebTA user accounts on a periodic basis. Management indicated that in order to gain access to WebTA, users first have to access AIDNet. Since, WebTA is a single sign on using AIDNet, users must recertify their accounts with AIDNet in order to continue using the application. As a result, management was not performing recertification of user accounts.

- Identified two of 336 separated employee accounts that were not disabled from WebTA after the individuals left USAID. Upon notification of the issue, USAID took action to correct this weakness.

- WebTA session termination setting was set to 30 minutes instead of the USAID policy requirement of 20 minutes. Management indicated that the setting had always been set to 30 minutes and was not aware of the policy requirement. Upon notification of the issue, USAID took action to correct this weakness.

By not ensuring that access request forms have been completed and approved along with not performing account recertification to review user accounts for appropriateness, there is an increased risk of granting inappropriate access to critical system resources. In addition, by not ensuring an appropriate session termination setting is in place, there is an increased risk of exposure for an unauthorized user to access critical system resources.

For the weaknesses related to terminated employees and session lock setting, management took action to correct the weaknesses. Therefore, we are not making recommendations at this time. However, we recommend the following for the remaining weaknesses:

> ***Recommendation 10:*** *We recommend that the chief information officer, in coordination with the chief financial officer, document and implement a procedure to complete, approve, and maintain access request forms for webTA users in accordance with policies, or document acceptance of the risk of not having such controls.*
>
> ***Recommendation 11:*** *We recommend that the chief information officer, in coordination with the chief financial officer, document and implement a procedure to review webTA accounts periodically for appropriateness in accordance with policies or document acceptance of the risk of not having such controls.*

7. USAID Needs to Strengthen the Plan of Action and Milestones Process

NIST Special Publication 800-53, Revision 4, security control CA-5, states the following regarding plan of action and milestones:

> The organization:
>
> * * *
>
> b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

For 16 of 24 AIDNet open plan of action and milestones (POA&M), USAID did not have justifications or an explanation for missing due dates. USAID did not have a process in place to assure POAMs were properly maintained and corrective action was taken in a timely manner. USAID utilizes the Cyber Security Asset Management (CSAM) system to create and maintain POA&Ms. However, when the "Delay Reason" is selected, CSAM did not require users to enter comments within the "Comments" section and USAID did not require comments to be entered for past due items. Furthermore, management indicated that the agency transitioned to the Risk Management System (RMS) in 2013 to facilitate the SA&A process including the tracking of POA&Ms. A decision was made to revert back to CSAM system in 2015. As a result, there was a gap in migrating POA&Ms back into CSAM and updating them accordingly. Upon notification of the issue, management updated the 16 delayed POA&Ms to reflect their current status.

By not properly updating POA&Ms to reflect their current status, USAID is unable to effectively monitor on-going system security risks. As a result, we recommend the following:

> ***Recommendation 12:*** *We recommend that the chief information officer develop and implement a written process to validate that the AIDnet plan of action and milestones is completed and updated promptly.*

8. USAID Needs to Strengthen Personnel Out-Processing Procedures

NIST Special Publication 800-53, Revision 4, security control PS-4, states the following regarding personnel termination:

> The organization, upon termination of individual employment:
>
> a. Disables information system access within [Assignment: organization-defined time period];
> b. Terminates/revokes any authenticators/credentials associated with the individual;
> c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
> d. Retrieves all security-related organizational information system-related property;

e. Retains access to organizational information and information systems formerly controlled by terminated individual; and
f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

USAID ADS 451 Mandatory Reference, *Separation and Exit Clearance Process,* dated April 21, 2016, states:

- The AMS is responsible for providing the AID 451-1 form to the separating employee at least 10 business days in advance of departure along with the Employment Search and Post-Employment Guidance, the link to take the Exit Survey, and instructions on the Exit Interview. More information on the Exit Survey and the Exit Interview can be found in 451.3.5 and 451.3.6, respectively.
- After SEC's certification of the AID 451-1 form, the separating employee takes the form to the HCTM Records Center for filing and transmission to the Payroll Office for processing any final pay due to the employee.

Controls were not adequate to ensure USAID effectively managed terminated employees. Specifically, we noted that seven of the 25 sampled separated employees from a total population of 336 separated employees, did not have an exit clearance form on file. In addition, two of the 25 sampled separated employees AIDNet user accounts were not disabled after the individuals left USAID.

The CIO Office and system owners did not consistently receive exit forms from Human Resources, Contracting Officer Representatives (CORs) and Administrative Management Staff (AMS) Officers that would be required to assure full exit notification and system account removal when employees and contractors leave the agency.

By not ensuing the employee separation process was completed properly, including the completion of all necessary documentation, collection of all organization property (badges, keys, keycards, etc.), and revocation of all employee access, USAID's security as well as information integrity may become compromised.

Recommendations addressing the findings were made in the fiscal year 2014[5] and fiscal year 2015 FISMA audits;[6] however, USAID had closed the recommendations. Therefore, we recommend the following:

> ***Recommendation 13:*** *We recommend that the director of the Office of Management Policy, Budget, and Performance, in coordination with the chief information officer and the chief human capital officer, document and implement a procedure to promptly remove system accounts associated with people no longer at the Agency.*

[5] Recommendation 18, *Audit of USAID's Fiscal Year 2014 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-000-15-003-P, October 30, 2014).
[6] Recommendation 2, *Audit of USAID's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-000-15-010-P, September 25, 2015).

Recommendation 14: *We recommend that the chief information officer, in coordination with the chief human capital officer, document and implement a process to verify that all employees' exit clearance forms are completed and maintained in accordance with policy.*

9. Physical Access Controls Surrounding Information Technology Rooms Need Improvement

NIST Special Publication 800-53, Revision 4, security control PE-2, states the following regarding physical access authorization:

The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and
d. Removes individuals from the facility access list when access is no longer required.

Of the 127 personnel with access to the IT rooms[7] at the Ronald Reagan Building and Two Potomac Yard locations, seven of a sample of 12 personnel did not have an approved access request on file. In addition, management indicated that no access recertification process was in place to ensure personnel still required access to the rooms. Upon notification of the issue, a spreadsheet completed by an AMS Officer on May 19, 2016 was provided; however, no corresponding approval evidence was provided for the remaining seven users.

To obtain access to IT rooms located within Ronald Reagan Building, an email is sent by the approved AMS Staff officer to the Office of Security (SEC) to grant access to specific IT rooms. The AMS officer coordinates with employee's supervisor/COR via email to retrieve necessary approvals for the access. For IT rooms located within the Two Potomac Yards facility there is a similar process except instead of sending an email to SEC, the AMS officer sends an email to Environment Protection Agency (EPA) to grant access to 2PY facility. Management indicated some of the users' access was granted several years ago and the initial approvals were not available. In addition, the point of contact was no longer with the respected agency, making it difficult to locate the access approvals.

By not ensuring effective physical access controls over USAID IT rooms, there is an increased risk of individuals gaining unauthorized access to USAID systems and data. As a result, we recommend the following:

Recommendation 15: *We recommend that the chief information officer document and implement a procedure to complete, approve, and maintain access request forms for individuals requiring access to the information technology rooms in the Ronald Reagan Building and Two Potomac Yard locations.*

[7] IT Room is where USAID houses switches, routers, UPC (back-up power) and telecommunication equipment.

Recommendation 16: *We recommend that the chief information officer document and implement a procedure to review individual access periodically and ensure only authorized personnel have access to information technology rooms in the Ronald Reagan Building and Two Potomac Yard locations.*

10. Information System Agreements Need to be Current

NIST Special Publication 800-53, Revision 4, security control CA-3, states the following regarding system interconnection:

> The organization:
> a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
> b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
> c. Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].

Controls were not adequate to ensure USAID had current memorandums of understanding and interconnection security agreements covering the interconnection between AIDNet and following entities:

- AIDNet and Office of Chief Financial Officer – National Finance Center, expired on January 22, 2016.
- AIDNet and the U.S. Department of Treasury Enterprise Business Solutions (EBS), expired on December 5, 2015.
- AIDNet and the Overseas Post Local Interconnection of Department of State Opennet, AIDNet expired in October 2012. Management indicated that this was no longer a connection and it would be removed from the AIDNet System Security Plan.
- Office of Foreign Disaster Assistance and USAID Chief Information Officer, expired on May 17, 2016.

USAID did not have a process in place to ensure memorandums of understanding and interconnection security agreements were reviewed and monitored on a periodic basis. Management indicated that the memorandum of understanding and interconnection security agreements were being tracked, but had not been signed yet due to changes in responsibility and oversight. A goal had been established to extend all agreements by the end of the fiscal year.

Without a current agreement, there is an increased likelihood of one party not properly protecting information or reporting security incidents to appropriate personnel. As a result, we recommend the following:

Recommendation 17: *We recommend that the chief information officer document and implement a validation process to confirm that all memorandums of understanding and interconnection security agreements are current and approved.*

11. USAID's Monitoring of Third Party Providers Needs to be Strengthened

NIST Special Publication 800-53, Revision 4, security control AC-20, states the following regarding use of external information system:

> Control Enhancements:
> (1) Use of External Information System | Limits on Authorized Use
> The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
> (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

NIST SP 800-35, *Guide to Information Technology Security Services*, the six phases of the IT security life cycles, Phase 5 states:

> Operations—the organization ensures operational success by consistently monitoring service provider and organizational security performance against identified requirements, periodically evaluating changes in risks and threats to the organization and ensuring the organizational security solution is adjusted as necessary to maintain an acceptable security posture.

The Enterprise Loan Management System (ELMS) is an external system that USAID contracted with Midland Loan Services, a division of PNC Financial Services Group Inc., to handle administration of loans and foreign currency transactions with USAID's financial portfolio. The Midland Loan Services, Service Organization Control (SOC 1) Type II Audit Report under Statement on Standards for Attestation Engagements No. 16 (SSAE 16) noted the following complementary user entity controls that need to be implemented by user organizations, such as USAID.

- Clients establish and maintain information security policies and procedures that provide for the overall direction and implementation of security controls at their company.
- Client personnel with access to the application are current and valid personnel, and access is appropriate based on employees' job responsibilities.
- Clients review reports sent by Midland, as applicable, regarding status of inactive user IDs (i.e., disable and/or deletion) and communicate action to be taken by Midland on a timely basis

Controls were not adequate to ensure USAID effectively implemented complementary user entity controls for the ELMS system. Specifically, we noted the following regarding ELMS account management controls:

- USAID did not have a fully documented access control procedure for ELMS describing how ELMS access is approved, disabled, and reviewed. The access control procedure only noted how a user requests access for ELMS.
- Accounts were not consistently deactivated after a period of inactivity. Specifically, 16 out of a population of 18 ELMS user accounts had not logged into the system for more than 90 days but remained active.

USAID did not have a process in place to ensure complementary entity user controls were implemented and monitored. Management indicated that ELMS was limited to reporting access and no transactions were entered or processed within ELMS by USAID staff since the accounting function had been contracted to Midland.

The lack of review of SSAE 16 reports for third party service providers can lead to the inability to realize the impact of control failures for the third party providers with respect to the adequacy of USAID's system of internal controls. In addition, management is not modifying and/or adding compensating controls as necessary to address the risk associated with identified weaknesses. As a result, we recommend the following:

> ***Recommendation 18:*** *We recommend that the chief financial officer document and implement a procedure to review third-party assessment reports to ensure complementary user entity controls have been implemented for the Enterprise Loan Management System.*
>
> ***Recommendation 19:*** *We recommend that the chief financial officer document and implement a procedure to review active Enterprise Loan Management System accounts that have not been used for a specified period and disable them as necessary in accordance with agency policy.*

12. USAID's Monitoring of the Phoenix Application Needs to be Strengthened

NIST Special Publication 800-53, Revision 4, security control SA-9, states the following regarding use of external information system

> The organization:
> * * *
> c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

NIST SP 800-35, *Guide to Information Technology Security Services*, the six phases of the IT security life cycles, Phase 5 states:

> Operations—the organization ensures operational success by consistently monitoring service provider and organizational security performance against identified requirements, periodically evaluating changes in risks and threats to the organization and ensuring the organizational security solution is adjusted as necessary to maintain an acceptable security posture.

In addition, Service Level Agreement (SLA) USAID and the U.S. Department of State (DoS), section *6.5 Security*, states, "Vulnerability scanning is performed on a weekly basis. The results are published in iPost, which USAID can access for review. The system owner can request an ad hoc scan through the CGFS ISSO."

The Phoenix Financial System is USAID's core financial management system that is hosted on the DoS network. According to the SLA between DoS and USAID,

vulnerability scanning of the system is the responsibility of DoS. As part of the SLA, USAID has the ability to monitor DoS to ensure vulnerability scanning is performed on a weekly basis, review the scan results, and ensure DoS is implementing corrective actions. However, USAID Phoenix management did not have a process to review DoS scan results on a periodic basis to identify known vulnerabilities in the Phoenix system. Specifically, Phoenix management did not provide evidence that scans were reviewed by USAID during the audit period. Management indicated that vulnerability scans are reviewed when an exception or incident occurs. In addition, management said they rely on DoS for continuous monitoring and for DoS to notify USAID when an incident occurs. The lack of review of vulnerability scan results for external information system on an on-going basis can lead to the inability to protect the Phoenix system from known vulnerabilities. In addition, unmitigated vulnerabilities on the Phoenix system can compromise the confidentiality, integrity, and availability of information within Phoenix system. As a result, we recommend the following:

> ***Recommendation 20:*** *We recommend that the chief financial officer document and implement a procedure to periodically review the Department of State vulnerability scan results and remediation actions supporting the Phoenix application.*

13. USAID Needs to Implement Controls Surrounding Role-based Training

NIST Special Publication 800-53, Revision 4, security control AT-3, states the following regarding role-based security training:

> The organization provides role-based security training to personnel with assigned security roles and responsibilities:
>
> a. Before authorizing access to the information system or performing assigned duties;
> b. When required by information system changes; and
> c. [Assignment: organization-defined frequency] thereafter.

In addition, ADS Chapter 545, states, "USAID employees, staff, contractors, or others working on behalf of USAID with significant security responsibilities (e.g., ISSOs and SAs) must receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities. When access to an Information system is contractual the COR must ensure that contractors complete the appropriate specialized training and refresher courses."

A role-based training program was not in place for personnel with the significant information security responsibilities. USAID plans to implement Workforce Skills Improvement Program for its dedicated IT security professionals. The program will document requirements and guidelines for information security-related education and skills improvement, however; the program was not fully implemented at the time of the audit.

By not ensuring role-based training, individuals responsible for system administration and security of USAID information systems may not maintain the knowledge required to perform their responsibilities.

A recommendation addressing this finding was made in the fiscal year 2015 audit;[8] however, procedures were not fully implemented and USAID had not closed the recommendation. Therefore, we are not making additional recommendations at this time.

[8] Recommendation 13, *Audit of USAID's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-000-15-010-P, September 25, 2015).

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the U.S. Agency for International Development (USAID) outlined its plans to address all 20 recommendations and described planned actions to address the recommendations. USAID's comments are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge management decisions on recommendations 1 through 20, though we disagree with the decisions for recommendations 1, 3 and 15. In addition, we acknowledge management's decision on recommendation 6; but we disagree that final action has been taken. Further, we acknowledge final action has been taken on recommendations 2, 12 and 14.

In response to recommendation 1, USAID management noted applicable laws and provided its interpretation of those laws as related to the CIO's reporting structure. USAID noted that OMB Memorandum M-15-14, *Management and Oversight of Federal Information Technology,* cites an acceptable example of a CIO reporting to "the Secretary, or Deputy Secretary serving on the Secretary's behalf". However, that example specifically states that those agencies had implemented legislation allowing for this change. The full excerpt from OMB M-15-14 states the following:

> As required by the Clinger Cohen Act and left in place by FITARA, the CIO "shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter." This provision remains unchanged, though certain agencies have since **implemented legislation** under which the CIO and other management officials report to a COO, Undersecretary for Management, Assistant Secretary for Administration, or similar management executive; in these cases, to remain consistent with the Clinger Cohen requirement as left unchanged by FITARA, the CIO shall have direct access to the agency head (i.e., the Secretary, or Deputy Secretary serving on the Secretary's behalf) regarding programs that include information technology.

Based on the above, the only way USAID can avoid having the CIO report directly to the agency head is if USAID has legislative authorization similar to the other agencies OMB mentioned. Therefore, USAID could obtain this authority from Congress and allow its CIO to report to the assistant administrator for the Bureau of Management. However, by not ensuring that the CIO position reports directly to the USAID Administrator or Deputy Administrator, there is a risk that the CIO will face challenges in fully exercising the duties and responsibilities to implement an effective and efficient information technology program for the agency. In its response, USAID also provided examples of other federal agencies, which have CIOs who do not report to their Agency head and are non-compliant with the law. However, USAID is its own entity and the other agencies mentioned are not in the purview of this audit. Therefore, we disagree with USAID's management decision on recommendation 1 and request the Agency to reconsider it.

In response to recommendation 3, USAID stated that M/CIO has structured the Senior Executive Service (SES) Deputy CIO role so that it oversees the Cybersecurity Program and USAID/Washington IT Operations, with the majority of the Deputy CIO's time being spent overseeing the USAID Cybersecurity Program. However, according to FISMA, CISOs must have information security duties as their official primary duty. USAID did not provide any evidence of how it would verify and measure that the Deputy CIO's primary duties would be overseeing the Cybersecurity program and ensuring the agency is in compliance with FISMA. Therefore, we disagreed with USAID's management decision on recommendation 3 and would like the Agency to reconsider it.

In response to recommendation 15, USAID noted that the access authorization process requires an email request be sent from an individual's AMS officer to SEC or EPA to provision physical access to USAID's server rooms in RRB or PY2, and that the request be maintained on file by the AMS officer. However, as noted in Finding 10, seven of a sample of 12 personnel did not have an approved access request on file. In addition, USAID noted that some of the sampled personnel had access prior to fiscal year 2016 and may have undergone a different provisioning process; however, no evidence of their access approval was provided, including a recertification of access. Therefore, we disagreed with USAID's management decision on recommendation 15 and would like the Agency to reconsider it.

In response to recommendation 6, USAID noted that M/CIO has implemented the use of a Nessus Vulnerability Scanner within the agency's network environment and that the tool has been configured in a similar capacity to the OIG's version. The Agency also said that recent internal scans utilizing Nessus had detected the same vulnerabilities identified by the OIG, which had been previously undetected. Therefore, the Agency requested the recommendation be closed upon issuance of the final report. We acknowledge USAID's management decision on Recommendation 6. However, because the Nessus tool was not fully implemented and configured at the time of our testing and to ensure the control is in place and operating effectively, an independent verification of the tool has to be done through an independent scan and configuration assessment. Therefore, final action has not yet been completed on recommendation 6.

In response to recommendation 2, USAID noted that the Agency has already developed a written plan to ensure that the CIO has a significant role in the overall resource and oversight processes related to IT procurements as mandated by FITARA. Key components of the plan include the development of standardized contract clauses, the creation of an Agency working group to determine how to best implement FITARA requirements, and the issuance of Agency-wide budget guidance requiring the identification of planned IT purchases. Specifically, on May 3, 2016, M/OAA released Acquisition and Assistance Policy Directive (AAPD 16-02) that requires the inclusion of a new IT clause in USAID contracts with planned IT procurements, requiring the review and approval of contracts for information technology or information technology services. Therefore, we acknowledge final action has been taken on recommendation 2.

In response to recommendation 12, USAID noted that M/CIO/IA has developed and implemented the *USAID POA&M Management Guide*, which provides system owners with the necessary guidance to identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in information systems. In addition, Information Assurance staff will request confirmation from the Information System

Security Officer and/or system owner that POA&Ms have been reviewed and updated. Further, the specific exceptions noted were remediated during the audit period. Therefore, we acknowledge final action has been taken on recommendation 12.

In response to recommendation 14, USAID noted several efforts were implemented to address the use of exit clearance forms for separating individuals, including sending agency-wide notices, updating the *Separations and Exit Clearance* policy, and implementing a tool to send automated emails notifying system owners that an individual has left the agency. In addition, USAID provided explanations and exit clearance forms for the remaining sampled separated employees. Therefore, we acknowledge final action has been taken on recommendation 14.

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 whether USAID implemented selected security controls for selected information systems[9] in support of the Federal Information Security Modernization Act of 2014.

The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* We assessed USAID's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Personnel Security
- Planning
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Services Acquisition

For this audit, we reviewed the following systems:

- Agency for International Development Network (AIDNet)
- Phoenix Financial System (Phoenix)
- Global Acquisition and Assistance System (GLAAS)
- WebTA (Web-based Time & Attendance)
- Enterprise Loan Management System (ELMS)

See Appendix IV for a listing of selected controls for each system.

[9] See Appendix IV for a list of systems and controls selected.

The audit also included an assessment of USAID's process for identifying and correcting/mitigating technical vulnerabilities on the USAID network (AIDNet.) The assessment included performing vulnerability assessment and penetration testing for USAID/Washington and four selected overseas missions (Ghana, Thailand, Georgia and El Salvador). In addition, a wireless assessment was conducted for the Ronald Reagan Building and Two Potomac Yard USAID locations.

The audit also included a follow up on prior audit recommendations[10] to determine if USAID made progress in implementing the recommended improvements concerning its information security program. The audit fieldwork was performed at the USAID offices in Washington, D.C. and Arlington, VA from April 8, 2016, to September 12, 2016.

Methodology

To determine if USAID's information security program met FISMA requirements, we conducted interviews with USAID officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. We also reviewed documents supporting the information security program. These documents included, but were not limited to, USAID's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; and (5) change control documentation. Where appropriate, we compared documents, such as USAID's information technology policies and procedures, to requirements stipulated in National Institute of Standards and Technology special publications. In addition, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

In addition, we completed an analysis of USAID's process for identifying and correcting/mitigating technical vulnerabilities on the USAID network (AIDNet) and performed penetration testing, wireless scanning and internal vulnerability scanning of AIDNet. This included performing vulnerability assessment and penetration testing for USAID/Washington and four selected overseas missions (Ghana, Thailand, Georgia and El Salvador). In addition, a wireless assessment was conducted for the Ronald Reagan Building and Two Potomac Yard USAID locations. We also reviewed the status of FISMA audit recommendations for fiscal year 2015.

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.

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

MANAGEMENT COMMENTS

October 7, 2016

MEMORANDUM

TO: Assistant Inspector General for Audit, Thomas Yatsco

FROM: Jay Mahanand, Chief Information Officer

SUBJECT: Management Response to Draft Report on the Audit of USAID's Fiscal Year 2016 Compliance with the Federal Information Security Management Act of 2002 (Audit Report No., A-000-17-XXX-P dated September XX 2016)

Thank you for the opportunity to respond to the Draft Audit Report. This memorandum contains the management decisions for the Draft Report on the Audit of USAID's Compliance with the Federal Information Security Management Act for Fiscal Year 2016.

All supporting documentation referenced within this response is provided in conjunction with this memorandum as tabbed references. After consultation with the front office and statutory officers referenced in the draft report, and after conferring with USAID's Office of the General Council, the following are the preliminary management decisions and corrective actions regarding the proposed audit recommendations:

CC: M/AA Assistant Administrator for Management (Acting), Angelique Crumbly
M/CFO Chief Financial Officer, Reginald Mitchell
M/MPBP Director, Colleen Allen
HCTM Chief Human Capital Officer, Kimberly Lewis
AGC, Jun Jin

Tab A

Recommendation 1: We recommend that the Deputy Administrator develop and implement a plan to ensure the chief information officer position reports directly to the Administrator or deputy administrator as required by the Federal Information Technology Acquisition Reform Act of 2014 and the Clinger-Cohen Act of 1996. Alternatively, USAID may obtain authority from Congress to allow the chief information officer to report to the assistant administrator for the Bureau of Management.

USAID Management Decision: The Agency does not agree with this recommendation. USAID, on an annual basis, provides Congress with the Agency Financial Report. In that report, the Agency highlights program and operational performance and includes our organizational structure which shows the direct reporting line to the AA/M of the CIO, CFO, and SPE and the indirect reporting line of these regulatory officers to the Administrator. Congress has never raised any issues or questioned these lines of reporting. Additionally, our review of the applicable law, policies, and other Agency arrangements lead us to conclude that USAID management possesses a certain amount of discretion in establishing reporting lines from the CIO to the USAID Administrator. We highlight such laws, policies, and practices below:

- The **Paperwork Reduction Act** (PRA) (44 USC 3506) requires executive branch agencies to designate a CIO to manage government-wide information technology practices. PRA specifies that an agency CIO must report directly to the agency head.
- The **Clinger-Cohen Act (**Clinger-Cohen) **(**40 USC 1425(b)) specifically references/implements the PRA requirement for designating a CIO. However, Clinger-Cohen characterizes the CIO's engagement with personnel more broadly, saying that the CIO "provides advice and other assistance to the head of the executive agency and other senior management personnel." The statute then talks about two specific instances of CIO direct engagement with the head of the agency, namely (1) "advis[ing] the head of the agency" with regard to the disposition of programs [40 USC 1425(c)(2)], and (2) "report[ing] to the head of the agency" on IT resource management improvements.
- The **Federal Information Technology Acquisition Reform Act** (FITARA) (40 USC 11319) left intact the PRA/Clinger-Cohen language. OMB Memo M-15-14 (2014) provides implementation guidance to agencies for FITARA. The OMB policy underscores the need to ensure that the CIO has "direct access" to the agency head. However, the Memo also references that some agencies have their CIO report to senior management officials other than the agency head. The OMB memo specifically cites an acceptable example of a CIO reporting to "the Secretary, or Deputy Secretary serving on the Secretary's behalf" [OMB Memorandum No. M-15-14, Section E, Attachment A, Q1 (p. 15)].
- The **Federal Information Security Management Act** (FISMA) (44 USC 3541) emphasizes coordination with other senior agency officials and an annual report to the agency head on the effectiveness of information security measures. This language mimics both the generality and specificity of Clinger-Cohen.

  Taken together, it appears that the PRA's mandate about a CIO direct reporting requirement to the agency head is further refined by Clinger-Cohen's insistence on CIO advice/assistance to not only an agency head, but to other senior management as well. Clinger-Cohen is thus more inclusive about whom an agency CIO advises. While Clinger-Cohen does talk about direct engagement with an agency head, it does so specifically in the context of two carefully delineated circumstances (namely, IT program disposition and reporting on IT management improvements). FISMA similarly highlights a specific "annual" report requirement to the agency head. We posit that the legislation does not require complete direct reporting relationship from the CIO to the agency head beyond the two circumstances mentioned above.

While the more recent FITARA legislation did not rescind the PRA or Clinger-Cohen, OMB's FITARA implementation guidance acknowledges the existence of virtually identical agency real-life practice where a CIO reports through a high-level official (rather than directly to the Agency head). A brief review of other agency arrangements revealed the following: (1) the CIO of the Department of State reports to the Under Secretary for Management; (2) the CIO of the Department of Justice reports to the Assistant Attorney General for Administration; and (3) the CIO for the Department of Agriculture reports to the Assistant Secretary for Administration. Therefore, a number of cabinet-level agencies have embedded their CIO function within their respective management/administration unit in the exact same manner as USAID's current arrangement via the M/CIO to M/AA reporting line.

Based upon the full body of applicable law read together, FITARA implementation guidance issued by OMB, and the practice by a number of other agencies, USAID believes that the current reporting arrangement from M/CIO to M/AA is appropriate and is critical in ensuring the cohesiveness of the management platform in supporting the Agency's humanitarian and development and humanitarian mission.

Target Date: The Agency requests that this recommendation be closed upon issuance of the report based on the supporting documentation listed and included as attachments.

Recommendation 2: We recommend that the Deputy Administrator develop a written plan to ensure the Chief Information Officer has a significant role in the management, governance, and oversight processes related to information technology as required by the Federal Information Technology Acquisition Reform Act of 2014.

Management Decision: Management Decision: The Agency does not agree with this recommendation and believes it should be removed from the report. The Agency has already developed a written plan (provided at Tab X) to ensure that the CIO has a significant role in the overall resource and oversight processes related to IT procurements as mandated by FITARA. Key components of the plan include the development of standardized contract clauses, the creation of an Agency working group to determine how to best implement FITARA requirements, and the issuance of Agency-wide budget guidance requiring the identification of planned IT purchases. Specifically, on May 3, 2016, M/OAA released Acquisition and Assistance Policy Directive (AAPD 16-02) (Tab V) that requires the inclusion of a new IT clause in USAID contracts with planned IT procurements, requiring the review and approval of contracts for information technology or information technology services. M/CIO led an intra-Agency working group that developed recommendations for implementing FITARA. Thus, for the first time, M/CIO has cross-Agency buy-in to ensure that all new acquisition awards containing IT procurements, whether program or Operating Expense (OE) funded, would be submitted to the CIO for review and approval. As part of the Agency's annual budget formulation process, the guidance now requires that all Operating Units (e.g., Missions, Bureaus, and Independent Offices) identify as part of their submission all IT-related procurements of goods and services, that are then reviewed and ranked by the Information Technology Steering Subcommittee (Co-chaired by the CIO and an SDAA of a geographic or functional bureau) of the Management Operations Council for Administrator approval. Further, the USAID Administrator directly approves the resources that are allocated to the IT Cost Center, which is managed directly by the Agency CIO.

Target Date: The Agency requests that this recommendation be removed from the report.

Recommendation 3: We recommend that the Chief Information Officer implement a plan to segregate the Deputy Chief Information Officer and Chief Information Security Officer positions and appoint in writing a senior-level Chief Information Security Officer in accordance with the Federal Information Security Modernization Act.

Management Decision: M/CIO does not agree with this recommendation. M/CIO does not believe there is a separation of duties issue with the Deputy CIO and CISO functions being assigned to the same individual. Previous OIG recommendations stated that the role of the CISO needed to be elevated to a higher level in the organization. As a result, the AA/M provided an SES allocation and requested that the CIO create a Deputy CIO to provide oversight and management of the information security function. Further, the AA/M created a SFS Deputy CIO to manage privacy and overseas operations. M/CIO has structured the SES Deputy CIO role so that it oversees the Cybersecurity Program and USAID/W IT Operations, with the majority of the Deputy CIO's time being spent in overseeing the USAID Cybersecurity Program. These duties of the M/CIO Deputy CIO and CISO role are highly complementary. It should also be noted that the Deputy CIO is **not** a system owner.

The CISO role leads the creation and operation of the Agency's Cybersecurity Program. Within M/CIO, cybersecurity policies and procedures are implemented through the IT operations functions. M/CIO and M Bureau management believe that the two responsibilities of the USAID Deputy CIO and CISO are integral to the Agency's efforts to build a safe computing environment. Furthermore, there is no requirement set forth in FISMA that explicitly requires the separation of the Deputy CIO and CISO roles. The CIO has written designation of Mark Johnson as the CISO in accordance with the Federal Information Security Modernization Act (Tab Y).

Target Date: M/CIO requests that this recommendation be closed upon issuance of the report based on the supporting documentation listed and included as attachments.

Recommendation 4: We recommend that the Chief Information Officer remediate vulnerabilities on the network identified by the Office of Inspector General's contractor, as appropriate, or document acceptance of the risks of those vulnerabilities.

Management Decision: M/CIO will remediate vulnerabilities on the network identified by the Office of Inspector General's contractor or document acceptance of the risks of those vulnerabilities.

Target Date: March 31, 2017

Recommendation 5: We recommend that the Chief Information Officer document and implement a process to track and remediate persistent vulnerabilities timely, or document acceptance of the risk of those vulnerabilities.

Management Decision: M/CIO will document and implement a process to track and remediate persistent vulnerabilities, or document acceptance of the risk of those vulnerabilities.

Target Date: March 31, 2017

Recommendation 6: We recommend that the Chief Information Officer document and implement a process to ensure vulnerability assessment tools are configured to detect vulnerabilities previously not detected by internal scans.

Management Decision: M/CIO believes sufficient action has been taken to address this recommendation. M/CIO has implemented the use of Nessus Vulnerability Scanner within the agency's network environment. This is the same vulnerability scanning tool used by the OIG contractors that found vulnerabilities previously undetected by the nCircle IP360 tool. The Nessus tool has been configured in a similar capacity to the OIG's version, and recent internal scans utilizing Nessus has detected the same vulnerabilities identified by the OIG, which were previously undetected. Moving forward, M/CIO plans to continue to utilize nCircle IP360, as it is the required tool for implementation of the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program. However, until IP360 is configured in a way that is comparable to that of Nessus' capabilities, M/CIO will continue to utilize the Nessus vulnerability management tool in a complementary capacity to IP360, to ensure that adequate vulnerability identification and remediation activities occur appropriately. Evidence of the Nessus vulnerability scanner tools usage and configuration (Tab W) are attached as support.

Target Date: M/CIO requests that this recommendation be closed upon issuance of the report based on the supporting documentation listed and included as attachments.

Recommendation 7: We recommend that the Chief Information Officer document and implement a process to centrally manage printers and apply hardened security configurations prior to placing printers into the production environment.

Management Decision: M/CIO will document and implement a process to centrally manage printers and apply hardened security configurations prior to placing printers into the production environment.

Target Date: September 30, 2017

Recommendation 8: We recommend that the Chief Information Officer document and implement a written plan to ensure all internal and external systems have a current authority to operate.

Management Decision: M/CIO has already started the process of working with system owners on the status of each system's ATO and a plan to ensure they are assessed and active, and will document and implement a written plan to ensure all systems have a current ATO.

Target Date: September 30, 2017

Recommendation 9: We recommend that the Chief Information Officer, in coordination with the Chief Financial Officer, document and implement written procedures to minimize exposure of personally identifiable information within the Web-Based Time and Attendance system.

Management Decision: M/CIO, in coordination with M/CFO, will document and implement written procedures to minimize exposure of personally identifiable information within webTA.

Target Date: August 15, 2017

Recommendation 10: We recommend that the Chief Information Officer, in coordination with the Chief Financial Officer, document and implement written procedures to complete, approve, and maintain access request forms for users with access to Web-Based Time and Attendance system in accordance with policies or document acceptance of the risk of not having such controls.

Management Decision: M/CIO, in coordination with M/CFO, will document the current business processes for activating and deactivating user accounts in webTA.

Target Date: May 31, 2017

Recommendation 11: We recommend that the Chief Information Officer, in coordination with the Chief Financial Officer, document and implement written procedures to review Web-Based Time and Attendance system accounts periodically for appropriateness in accordance with policies or document acceptance of the risk of not having such controls.

Management Decision: M/CIO, in coordination with M/CFO, will document the current business processes for periodic review of users and associated user roles in webTA.

Target Date: March 31, 2017

Recommendation 12: We recommend that the Chief Information Officer develop and implement a written process to validate whether the plan of action and milestones are completed and updated timely.

Management Decision: M/CIO believes sufficient action has been taken to address this recommendation. M/CIO/IA has developed and implemented the *USAID POA&M Management Guide* (Tab T), which provides System Owners (SOs) with the necessary guidance to identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in information systems. Section 4.7, *Monitor and Update,* provides the following guidance for timely completion and updating of POA&Ms:

> *"POA&M data should be monitored and updated on a continuous basis, as events occur. USAID requires that all information in the POA&M be updated at least quarterly and be accurate as of the last day of each quarter for tracking and reporting.*
>
> *As part of their quarterly review, the IA staff and/or ISSO should validate that the weaknesses are properly identified and prioritized and that appropriate resources have been made available to resolve the weaknesses. Additionally, the ISSO and/or IA staff review must ensure that the schedule for resolving the weakness is both appropriate and achievable.*
>
> *Each quarter, IA staff will request confirmation from the ISSO and/or system owner that POA&Ms have been reviewed and updated. Selected systems will be*

manually reviewed by the IA staff to ensure that POA&Ms are being managed effectively. When issues are detected, the IA staff will request a meeting with the ISSO and/or system owner to discuss remedial actions. Monthly reports on POA&M status will be provided to the CISO and CIO."

Additionally, as noted in the audit report, the issue identified for the AIDNet POA&M has subsequently been remediated.

Target Date: M/CIO requests that this recommendation be closed upon issuance of the report based on the supporting documentation listed and included as attachments.

Recommendation 13: We recommend that the Director of the Office of Management Policy, Budget, and Performance, in coordination with the Chief Information Officer, and the Chief Human Capital Officer, document and implement a written procedures to promptly remove system accounts associated with people no longer at the agency.

Management Decision: M/CIO, in coordination with the Offices of Management Policy, Budget, and Performance (M/MPBP) and Human Capital and Talent Management (HCTM), will document and implement written procedures to promptly remove system accounts associated with people no longer at the Agency.

Target Date: March 30, 2017

Recommendation 14: We recommend that the Chief Information Officer in coordination with the Director, Office of Human Resources, document and implement a written process to verify that all employees' exit clearance forms are completed and maintained in accordance with policy.

Management Decision: M/CIO believes sufficient action has been taken to address this recommendation. During FY2015, several efforts were implemented to address the use of exit clearance forms for separating individuals, including but not limited to:

1. M/CIO issued Notice 30066 entitled "Information Technology Asset Management Employee Separation and Transfer Procedures" (Tab B), which provides policy and procedures for the management of information technology (IT) assets upon an employee's separation from the Agency or transfer to another USAID bureau, office, or mission. The policy applies to U.S. direct hires, U.S. personal services contractors, Foreign Service nationals, third country nationals, interns, and individuals detailed to USAID from another Federal agency.
2. M/CIO issued updated operational policy Automated Directives System (ADS) Chapter 451, "Separations and Exit Clearance" (Tab C), providing clear guidance on policy and procedures for employees and contractors separating from or moving within USAID, including procedures for removing system accounts. A new exit clearance form (AID 451-1 Tab D) and instructions accompanied this newly revised chapter.
3. M/CIO issued Notice 38156 entitled "Control of Information Technology (IT) Assets Provided to Institutional Contractors as Government Furnished Property (GFP)" (Tab E), which includes respective procedures for USAID/W and Mission officials for returning GFP for employees and contractors.
4. M/CIO utilizes ServiceNow as an IT Service Management tool, and has configured it to send automated emails to system owners notifying them that an

individual has left the Agency once an AMS officer has initiated the off-boarding process (Tab F). This automated email is part of the BSE notification that is assigned to the Application O&M Team to remove application accounts as appropriate (Tab G). An accompanying Standard Operating Procedure entitled "USAID Off-Boarding Process Workflow to Remove Accounts" (Tab H) was documented to describe and implement the off-boarding process utilizing the ServiceNow software.

Finally, USAID has obtained exit clearance forms for 4 of the 7 users sampled (Tabs I-L). One of the individuals in the sample never left the Agency; instead, they transferred from one mission to another within the same region (USAID/Tanzania to USAID/Kenya), and were subsequently captured in the system as a "separation" due to changing posts (Tab M-N). The remaining two individuals were on TDY for a month (Tab O) and a week (Tab P) respectively, and were not required to complete a checkout sheet.

Target Date: M/CIO requests that this recommendation be closed upon issuance of the report based on the supporting documentation listed and included as attachments.

Recommendation 15: We recommend that the Chief Information Officer document and implement written procedures to complete, approve, and maintain access request forms for individuals requiring access to the information technology rooms within the Ronald Reagan Building and Two Potomac Yard locations.

Management Decision: M/CIO believes this control was operating effectively. Evidence was provided for one of the seven individuals identified as not having approved physical access (Tabs Q-R) that was subsequently not accepted by the auditors due to the timeliness of providing the artifact. Furthermore, M/CIO has documented and implemented the *Operation and Maintenance of USAID's Information Technology Infrastructure and Systems Program, Computer and Network Room Access, Standard Operating Procedure (SOP)* (Tab S), which provides instructions required to obtain badged ID Card physical access to computer and network rooms in PY2, RRB, WLC, and CP3. This access authorization process requires an email request be sent from an individual's AMS officer to SEC or EPA to provision physical access to USAID server rooms in RRB or PY2, and is maintained on file by the AMS officer. M/CIO believes the current process is operating effectively, and addresses the need to complete, approve, and maintain an access request for physical access to server rooms. Outside of the one individual whose evidence was not accepted by the auditors, the remaining six individuals sampled were provisioned access prior to FY16, and may have undergone a different provisioning process.

Target Date: M/CIO requests that this recommendation be closed upon issuance of the report based on the supporting documentation listed and included as attachments.

Recommendation 16: We recommend that the Chief Information Officer document and implement a written procedures to ensure individual's access is reviewed periodically and only authorized personnel have access to Ronald Reagan Building and Two Potomac Yard locations.

Management Decision: M/CIO will document and implement a written procedure to ensure individual's access is reviewed periodically and only authorized personnel have access to Ronald Reagan Building and Two Potomac Yard locations.

Target Date: March 30, 2017

Recommendation 17: We recommend that the Chief Information Officer document and implement a written validation process to confirm the all memorandums of understanding and interconnection security agreements are current and approved.

Management Decision: M/CIO will document and implement a written validation process to confirm that all memorandums of understanding and interconnection security agreements are current and approved.

Target Date: March 30, 2017

Recommendation 18: We recommend that the Chief Financial Officer document and implement a written procedures to review third party assessment reports to ensure complementary user entity controls have been implemented for the Enterprise Loan Management System.

Management Decision: M/CFO will document and implement written procedures to review third party assessment reports to ensure complementary user entity controls have been implemented for Portfolio Insight.

Target Date: March 1, 2017

Recommendation 19: We recommend that the Chief Financial Officer document and implement a written procedures to review active Enterprise Loan Management System accounts that have not logged in over a specified period of time and disable as necessary in accordance with agency policy.

Management Decision: Portfolio Insight is owned and operated by Midland Loan Services, a division of PNC Financial Services, Inc. USAID tracks when USAID user access and user termination is requested. These are complementary controls that are implemented based on USAID's assessment of risk. Access is limited to reporting access, and no transactions are entered or processed by USAID staff. USAID does not have the authority or access to disable accounts and relies on Midland personnel to take action on account activation and termination requests by USAID. The Chief Financial Officer does not accept this recommendation as written, but will document and implement written procedures to review active Portfolio Insight accounts that have not logged in over a specified period of time and request that Midland deactivate inactive users, as requested by USAID.

Target Date: March 1, 2017

Recommendation 20: We recommend that the Chief Financial Officer document and implement a written procedures to review the Department of State vulnerability scan results and remediation actions supporting the Phoenix Application on a periodic basis.

Management Decision: M/CFO will update the procedures that are documented in the Department of State and USAID Service Level Agreement (SLA) to review Phoenix-related vulnerability scans and associated remediation actions on a periodic basis.

Target Date: April 30, 2017

CC M/CIO Chief Information Security Officer, Mark Johnson
M/CIO Information Assurance, William Morgan
M/CIO Audit Management Officer, Kenneth Kerttula

Tab B
Information Technology Asset Management Employee Separation and Transfer Procedures

Tab C
Automated Directives System (ADS) Chapter 451, "Separations and Exit Clearance

Tab D
New exit clearance form (AID 451-1)

Tab E
"Control of Information Technology (IT) Assets Provided to Institutional Contractors as Government Furnished Property (GFP)"

Tab F
Off-boarding process

Tab G
Application O&M Team to remove application accounts as appropriate

Tab H
"USAID Off-Boarding Process Workflow to Remove Accounts"

Tab I thru Tab L
Exit clearance forms

Tab M & Tab N
"Separation" due to changing post

Tab O
TDY for a month

Tab P
TDY for a week

Tab Q & Tab R
Individuals identified as not having approved physical access

Tab S

Operation and Maintenance of USAID's Information Technology Infrastructure and Systems Program, Computer and Network Room Access, Standard Operating Procedure (SOP)

Tab T
USAID POA&M Management Guide

Tab U
USAID Information Technology Acquisition Assessment and Authorization (ITAAA) Plan

Tab V
AAPD 16-02

Tab W
Evidence of the Nessus vulnerability scanner tools usage and configuration
https://drive.google.com/file/d/0B3wTVdK2a7JlRWJnakRrdnZGLUk/view
*(Access request required as link contains sensitive information. M/CIO can provide access upon request)

Tab X
FITARA Implementation Plan

Tab Y
CISO Designation

Tab Z
SIGNED CFO Management Response to Draft Audit Report on FISMA 2016

Status of Prior Year Findings

The following table provides the status of the FY 2015 FISMA audit recommendations. [11]

No.	FY 2015 Audit Recommendation	USAID Status	Auditor's Position on Status
1	We recommend that the Chief Information Officer document and implement procedures to review active network accounts that have not logged in over a specified period of time, as defined by Automated Directives System Chapter 545, "Systems Security Policy," or that have never logged into the system to determine whether accounts are necessary and disable or delete accounts that are unnecessary.	Closed	Agree
2	We recommend that the Director of the Office of Management Policy, Budget, and Performance, in coordination with the Chief Information Officer, the Chief Human Capital Officer, and the Director of the Office of Acquisition and Assistance, document and implement procedures to promptly remove system accounts associated with people no longer at USAID.	Closed	Disagree. FY 2016 FISMA Audit noted weaknesses, Please refer to Finding 8.
3	We recommend that the Chief Information Officer implement improved procedures to make sure approved access request forms are maintained for anyone with access to the network.	Closed	Agree
4	We recommend that the Chief Information Officer work with the AIDtracker system owner to update AIDtracker security settings for user inactivity to comply with policy, or issue a written authorization for deviations.	Closed	Agree
5	We recommend that the Chief Information Officer work with the AIDtracker system owner to document and implement procedures to make sure approved access request forms are maintained for anyone with access to the system.	Closed	Agree
6	We recommend that the Director for the Office of Security document and implement procedures to review Partner Vetting System accounts that have not logged in over a specified period of time, as defined by USAID, or that have never logged into the system to determine whether accounts are necessary.	Open	Agree

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

No.	FY 2015 Audit Recommendation	USAID Status	Auditor's Position on Status
7	We recommend that the Chief Information Officer work with the State Department's Director for the Office of U.S. Foreign Assistance Resources to implement procedures to complete, approve, and maintain approved access request forms for privileged users with access to the Foreign Assistance Coordination and Tracking System Info as required in accordance with policies.	Closed	Disagree. FACTS Info was not in scope for the FY 2016 FISMA Audit. Upon review of the closure package, we noted that no evidence was provided to display implementation of the recommendation. The closure package only included documented procedures.
8	We recommend that the Chief Information Officer work with the State Department's Director for the Office of U.S. Foreign Assistance Resources to document and implement procedures to review active Foreign Assistance Coordination and Tracking System Info accounts that have not logged in over a specified period of time or that have never logged into the system to determine whether accounts are necessary.	Closed	Disagree. FACTS Info was not in scope for the FY 2016 FISMA Audit. Upon review of the closure package, we noted that no evidence was provided to display implementation of the recommendation. The closure package only included documented procedures.
9	We recommend that the Chief Information Officer work with the State Department's Director for the Office of U.S. Foreign Assistance Resources to document and implement procedures to review Foreign Assistance Coordination and Tracking System Info accounts periodically for appropriateness.	Closed	Disagree. FACTS Info was not in scope for the FY 2016 FISMA Audit. Upon review of the closure package, we noted that no evidence was provided to display implementation of the recommendation. The closure package only included documented procedures.
10	We recommend that the Chief Information Officer conduct a full system reauthorization for the AIDtracker system in accordance with USAID's policy.	Closed	Agree
11	We recommend that the Chief Information Officer conduct a full system reauthorization for the Partner Vetting System in accordance with USAID's policy.	Open	Agree
12	We recommend that the Chief Information Officer implement a documented validation process to confirm that continuous monitoring activities—such as updating system security plans, risk assessments, security assessments, and plan of action and milestones—are occurring for all USAID systems on a periodic basis, as defined by USAID, and as significant system changes occur.	Open	Agree. FY 2016 FISMA Audit noted weaknesses, Please refer to Finding 4.

No.	FY 2015 Audit Recommendation	USAID Status	Auditor's Position on Status
13	We recommend that the Chief Information Officer document and implement a process to confirm that the role-based training program is implemented as applicable for all employees and contractors requiring role-based training, and be sure the training is tracked and documented.	Open	Agree. FY 2016 FISMA Audit noted weaknesses, Please refer to Finding 14.
14	We recommend that the Chief Information Officer update the AIDNet system security plan to fully document the system's security controls.	Closed	Agree
15	We recommend that the Director for the Office of Security implement a documented validation process to confirm that the Partner Vetting System contingency plan is reviewed, updated, and tested annually.	Open	Agree
16	We recommend that the Chief Information Officer document a formal memorandum of understanding with the alternate processing vendor.	Closed	Agree
17	We recommend that the Director for the Office of Security document, implement, test, and maintain a current, accurate baseline configuration for the Partner Vetting System.	Open	Agree

Summary of Results of Each Control Reviewed

Control	Control Name	Is Control Effective
AIDNET		
AC-1	Access Control Policy & Procedures	Yes
AC-2	Account Management	No, See Finding 8
AC-3	Access Enforcement	Yes
AC-4	Information Flow Enforcement	Yes
AC-5	Separation of Duties	Yes
AC-6	Least Privilege	Yes
AC-11	Session Lock	Yes
AC-12	Session Termination	Yes
AC-17	Remote Access	Yes
AC-19	Access Control for Mobile Devices	Yes
AC-20	Use of External Information Systems	No, See Finding 1 and 11
AT-1	Security Awareness & Training Policy and Procedures	Yes
AT-2	Security Awareness	Yes
AT-3	Role-Based Security Training	No, See Finding 13
AT-4	Security Training Records	Yes
AU-1	Audit & Accountability Policy and Procedures	Yes
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	No, See Finding 4
CA-3	Information System Connections	No, See Finding 10
CA-5	Plan of Action and Milestones	No, See Finding 7
CA-6	Security Authorization	No, See Finding 4
CA-7	Continuous Monitoring	Yes
CM-1	Configuration Management Policy & Procedures	Yes
CM-2	Baseline Configuration	Yes
CM-3	Configuration Change Control	Yes
CM-4	Security Impact Analysis	Yes
CM-6	Configuration Settings	Yes
CM-7	Least functionality	Yes
CM-8	Information System Component Inventory	Yes
CP-1	Contingency Planning Policy & Procedures	Yes

Control	Control Name	Is Control Effective
CP-2	Contingency Plan	Yes
CP-3	Contingency Training	Yes
CP-4	Contingency Plan Testing and Exercises	Yes
CP-6	Alternate Storage Sites	Yes
CP-7	Alternate Processing Sites	Yes
CP-8	Telecommunication Services	Yes
CP-9	Information System Backup	Yes
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	Yes
IR-1	Incident Response Policy and Procedures	Yes
IR-4	Incident Handling	Yes
IR-5	Incident Monitoring	Yes
IR-6	Incident Reporting	Yes
IR-8	Incident Response Plan	Yes
PE-2	Physical Access Authorizations	No, See Finding 9
PE-3	Physical Access Control	Yes
PL-2	System Security Plan	Yes
PL-4	Rules of Behavior	Yes
PS-6	Access Agreements	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	No, See Finding 4
RA-5	Vulnerability Scanning	No, See Finding 3
SA-1	System & Services Acquisition Policy and Procedures	Yes
SA-9	External Information System Services	Yes
SC-1	System & Communications Protection Policy & Procedures	Yes
SC-7	Boundary Protection	Yes
SC-8	Transmission Integrity	Yes
SI-2	Flaw Remediation	No, See Finding 3
PM-1	Information Security Program Plan	Yes
PM-3	Information Security Resources	Yes
PM-4	Plan of Action and Milestones Process	No, See Finding 7

Control	Control Name	Is Control Effective
PM-5	Information System Inventory	Yes
PM-6	Information Security Measures of Performance	Yes
PM-7	Enterprise Architecture	Yes
PM-8	Critical Infrastructure Plan	Yes
PM-9	Risk Management Strategy	Yes
PM-10	Security Authorization Process	Yes
PM-12	Insider Threat Program	Yes
Phoenix		
AC-1	Access Control Policy & Procedures	Yes
AC-5	Separation of Duties	Yes
AC-11	Session Lock	Yes
AU-2	Audit Events	Yes
AU-3	Content of Audit Records	Yes
AU-4	Audit Storage Capacity	Yes
AU-5	Response to Audit Processing Failures	Yes
CA-2	Security Assessments	Yes
CA-5	Plan of Action and Milestones	Yes
CA-6	Security Authorization	Yes
CM-2	Baseline Configuration	Yes
CM-8	Information System Component Inventory	Yes
CP-6	Alternate Storage Sites	Yes
CP-9	Information System Backup	Yes
PL-2	System Security Plan	Yes
PL-4	Rules of Behavior	Yes
PS-6	Access Agreements	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	No, See Finding 12
SA-1	System & Services Acquisition Policy and Procedures	Yes
SA-9	External Information System Services	Yes
GLAAS		
AC-1	Access Control Policy & Procedures	Yes
AC-5	Separation of Duties	Yes
AC-11	Session Lock	Yes
CA-5	Plan of Action and Milestones	Yes
CA-6	Security Authorization	Yes
CM-1	Configuration Management Policy & Procedures	Yes

Control	Control Name	Is Control Effective
CM-8	Information System Component Inventory	Yes
CP-1	Contingency Planning Policy & Procedures	Yes
CP-6	Alternate Storage Sites	Yes
CP-9	Information System Backup	Yes
PL-2	System Security Plan	Yes
PL-4	Rules of Behavior	Yes
PS-6	Access Agreements	Yes
RA-2	Security Categorization	Yes
SA-1	System & Services Acquisition Policy and Procedures	Yes
SA-9	External Information System Services	Yes
WebTA		
AC-1	Access Control Policy & Procedures	Yes
AC-5	Separation of Duties	Yes
AC-11	Session Lock	No, See Finding 6
CA-5	Plan of Action and Milestones	Yes
CA-6	Security Authorization	Yes
CM-1	Configuration Management Policy & Procedures	Yes
CM-8	Information System Component Inventory	Yes
CP-1	Contingency Planning Policy & Procedures	Yes
CP-6	Alternate Processing Sites	Yes
CP-9	Information System Backup	Yes
PL-2	System Security Plan	No, See Finding 4
PL-4	Rules of Behavior	Yes
PS-6	Access Agreements	No, See Finding 6
RA-2	Security Categorization	Yes
SA-1	System & Services Acquisition Policy and Procedures	Yes
SA-9	External Information System Services	Yes
ELMS		
AC-1	Access Control Policy & Procedures	No, See Finding 11
AC-2	Account Management	No, See Finding 11
AC-5	Separation of Duties	Yes
AC-7	Unsuccessful Login Attempts	Yes
AU-11	Audit Record Retention	Yes
CA-2	Security Assessments	Yes
CA-5	Plan of Action and Milestones	Yes
CA-6	Security Accreditation	Yes
CA-7	Continuous Monitoring	Yes

Control	Control Name	Is Control Effective
CM-4	Security Impact Analysis	Yes
CM-9	Configuration Management Plan	Yes
CP-1	Contingency Planning Policy & Procedures	Yes
CP-9	Information System Backup	Yes
RA-2	Security Categorization	Yes
SA-9	External Information System Services	Yes
SI-4	Information System Monitoring	Yes
SI-10	Information Input Validation	Yes

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. AA101316