OFFICE OF INSPECTOR GENERAL

U.S. Agency for International Development

USAID Has Gaps in Conforming With the Federal Information Technology Acquisition Reform Act

AUDIT REPORT A-000-19-004-C
NOVEMBER 9, 2018

1300 Pennsylvania Avenue NW • Washington, DC 20523
https://oig.usaid.gov • 202-712-1150

Office of Inspector General, U.S. Agency for International Development

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, U.S. African Development Foundation, Inter-American Foundation, Millennium Challenge Corporation, and Overseas Private Investment Corporation.

Report waste, fraud, and abuse

USAID OIG Hotline
Email: ig.hotline@usaid.gov
Complaint form: https://oig.usaid.gov/complainant-select
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: November 9, 2018

TO: USAID, Acting Deputy Administrator, David H. Moore

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

SUBJECT: USAID Has Gaps in Conforming With the Federal Information Technology Acquisition Reform Act (A-000-19-004-C)

Enclosed is the final audit report on the U.S. Agency for International Development's (USAID) implementation of the Federal Information Technology Acquisition Reform Act (FITARA). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm Brown & Company CPAs and Management Consultants PLLC (Brown & Company) to conduct the audit. The contract required Brown & Company to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed Brown & Company's report and related audit documentation and inquired of its representatives. The audit firm is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which Brown & Company did not comply, in all material respects, with applicable standards.

The objective of this performance audit was to determine whether USAID established a framework for the management and oversight of its information technology as prescribed by FITARA. Specifically, the audit sought to determine whether USAID established a comprehensive plan to implement Federal requirements for the management and oversight of its information technology, as required by Office of Management and Budget (OMB) M-15-14, "Management and Oversight of Federal Information Technology," June 10, 2015.

To answer the audit objective, Brown and Company reviewed USAID's FITARA Common Baseline Implementation Plan and information technology (IT) strategic and operational plans; management policies, procedures, processes, and practices for IT investments; and IT governance and control practices related to the implementation of FITARA. In addition, Brown and Company obtained an understanding of the internal controls over the implementation of FITARA through interviews and observations, as well as through inspections of documents including organizational policies and procedures. Audit fieldwork was performed at USAID's headquarters in Washington, DC, from November 18, 2016, through December 13, 2017.

Brown & Company concluded that USAID had not established a comprehensive framework to implement FITARA. Of the 23 applicable OMB M-15-14 common baseline requirements, USAID had implemented only 7:

- Assigned the chief information officer (CIO) a significant role as a member of governance boards that include IT resources.
- Standardized cost savings metrics and performance indicators as part of the reporting requirements for Integrated Data Collection.
- Provided monthly reports to the Federal IT Dashboard on risks, performance metrics, and project and activity data for major IT investments as soon as the data became available, or at least once each calendar month.
- Held PortfolioStat sessions quarterly with OMB, the agency CIO, and other attendees.
- Sent annual Acquisition Human Capital Plans to OMB's Office of Federal Procurement Policy in support of IT acquisition cadres.
- Adhered to category management[1] and the Federal Strategic Sourcing Initiative (FSSI), which requires agencies to comply with an upcoming OMB rule when using another mechanism to purchase services and supplies that are offered under an FSSI agreement.
- Used a Governmentwide program to purchase enterprise software licenses for new awards as a part of category management.

However, USAID did not establish a comprehensive FITARA Common Baseline Implementation Plan that identified actions needed to address the remaining requirements in the following areas.

CIO Reporting Arrangement

The CIO needs to report directly to the Administrator or Deputy Administrator as required by OMB M-15-14 and the Clinger-Cohen Act of 1996. In management comments on a prior audit report,[2] Agency officials took the position that the CIO is not required to report to the Agency head. However, OMB's position is that only agencies with a statutory exception to Clinger-Cohen may direct their CIOs to report to specified lower-level officials if those agencies allow the CIO to have "direct access" to the agency head or deputy agency head. However, USAID's CIO does not report directly to the Agency head, and the Agency does not have a statutory exception that allows the CIO to report to a lower-level Agency official.

[1] According to OMB M-15-14, category management is the management of spending by categories such as IT and transportation. It is designed to help agencies avoid duplicative spending.
[2] "USAID Has Implemented Controls in Support of FISMA, but Improvements Are Needed" (A-000-17-001-C), October 27, 2016,

We therefore recommend that USAID:

Recommendation 1. Develop and implement a governance structure so that the chief information officer position reports directly to the Administrator as required by the Federal Information Technology Acquisition Reform Act and the Clinger-Cohen Act.

CIO Authority

The CIO needs authority for:

- Formulating and executing the IT budget.
- Overseeing the management of IT resources across the Agency and its programs. The CIO needs oversight along with appropriate involvement in the management of the Agency's IT resources to enforce transparency and meet authorization-to-operate requirements.
- Enforcing a complete, accurate IT inventory of the Agency's data centers, IT investments, and FISMA reportable systems to govern IT across the Agency.

We therefore recommend that USAID:

Recommendation 2. Revise Automated Directives System 101 to give the chief information officer the roles, responsibilities, and authorities to oversee all annual and multiyear planning, programming, and budget execution decisions, and reports related to information technology resources, as required by the Federal Information Technology Acquisition Reform Act.

Recommendation 3. Develop and implement policies that give the chief information officer authority for formulating and executing the information technology budget and overseeing information technology resources, as required by the Federal Information Technology Acquisition Reform Act.

Recommendation 4. Revise Agency policies and procedures to provide the chief information officer with information needed for overseeing all information technology investments and acquisitions to prevent, detect, and correct shadow and hidden information technology.

Recommendation 5. Issue a written decision on whether to authorize DTRAMS, and take appropriate actions to comply with security assessment and authorization controls in National Institute of Standards and Technology Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."[3]

[3] DTRAMS is a travel data collection system for the Democracy, Conflict and Humanitarian Assistance Bureau.

Recommendation 6. Document and implement an inventory validation process to accurately and completely document information technology investments, the information technology systems inventory, and the Federal Information Security Modernization Act reportable systems inventory.

Recommendation 7. Document and implement processes for maintaining accurate records for, and managing the consolidation and streamlining of, its information technology resources, systems, data centers, and other shared information technology services in compliance with Office of Management and Budget Memorandum M-15-14.

FITARA Definitions for IT and IT Resources

USAID has not adopted the FITARA definitions for IT and IT resources. We therefore recommend that USAID:

Recommendation 8. Revise Agency policies, procedures, and directives to adopt the definitions of terms and requirements presented in Office of Management and Budget Memorandum M-15-14, including (1) information technology budgetary resources, personnel, and facilities and (2) acquisitions and interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements.

Staff Competency

USAID needs to enforce the competency requirements for IT staff. We therefore recommend that USAID:

Recommendation 9. Document and implement a process to enforce the competency requirements for information technology staff, including those in information technology leadership positions, and complete the assessment of competency requirements for information technology staff.

In finalizing the report, Brown & Company evaluated USAID's responses to the recommendations. We reviewed that evaluation, and we consider recommendations 2, 7, and 8 closed; recommendations 1, 3, 4, 5, and 9 resolved but open pending completion of planned activities; and recommendation 6 open and unresolved because USAID was not able to demonstrate that it has an inventory validation process that traces IT investments to IT systems and FISMA-reportable systems.

For recommendations 1, 3, 4, 5, and 9, please provide evidence of final action to the Audit Performance and Compliance Division. Please work with us to resolve recommendation 6.

We appreciate the assistance extended to our staff and Brown & Company employees during the engagement.

cc: Acting Assistant Administrator, A-AA/M, Angelique M. Crumbly
Chief Information Officer, M/CIO, Jay Mahanand
Chief Human Capital Officer, William R. Leavitt

USAID HAS GAPS IN CONFORMING WITH THE FEDERAL INFORMATION TECHNOLOGY ACQUISITION REFORM ACT (FITARA)

Final Report
October 17, 2018

Submitted by:

Brown & Company CPAs and Management Consultants, PLLC
1101 Mercantile Lane, Suite 122
Largo, MD 20774

USAID HAS GAPS IN CONFORMING WITH THE FEDERAL INFORMATION TECHNOLOGY ACQUISITION REFORM ACT (FITARA)

Table of Contents

1. **INTRODUCTION** 1
2. **BACKGROUND** 2
3. **SUMMARY OF RESULTS** 3
4. **DETAILED FINDINGS** 4

FINDING 1 – The FITARA Implementation Plan Did Not Fully Address the Need for the CIO to Report Directly to the Administrator as Required by OMB M-15-14 and the Clinger-Cohen Act…….. 4

FINDING 2 – The FITARA Implementation Plan Did Not Fully Address the Need for USAID to Adopt the FITARA Definition For IT Resources. 6

FINDING 3 – The FITARA Implementation Plan Did Not Fully Address the Need for the CIO to Have Adequate Oversight and Decision Authority Over All Budget Execution Activities Related to the Evaluation of IT Resources, Planned Expenditures, and Governance Around IT Policies and Procedures. 8

FINDING 4 – The FITARA Implementation Plan Did Not Fully Address the Need for the CIO to Have Authority to Oversee IT Resources Across the Entire Agency and its Programs, and to Have Appropriate Visibility and Involvement in the Management and Oversight of IT Resources…….. 10

FINDING 5 – The FITARA Implementation Plan Did Not Address the Need for USAID's Policies to Provide the CIO with the Authorization to Carry Out Oversight and Decision Authority Over All Agency IT Implementations to Meet Authorization to Operate Requirements. 12

FINDING 6 – The FITARA Implementation Plan Did Not Address the Need for the CIO to Have Authorization to Enforce Transparency for the IT Inventory Across the Agency. 14

FINDING 7 – The FITARA Implementation Plan Did Not Address the Need for USAID to Maintain Accurate Records for Managing the Consolidation and Streamlining of Its IT Resources and Data Centers. 16

FINDING 8 – The FITARA Implementation Plan Did Not Fully Address the Need for the CIO and Chief Human Capital Officer to Enforce the Competency Requirements for IT Staff, Including IT Leadership Positions. 17

5. **EVALUATION OF MANAGEMENT COMMENTS** 19
6. **APPENDIX I – PURPOSE, OBJECTIVE, SCOPE AND METHODOLOGY** 23
7. **APPENDIX II – OMB M-15-14 COMMON BASELINE REQUIREMENTS** 25
8. **APPENDIX III – MANAGEMENT COMMENTS** 30

BROWN & COMPANY
CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

USAID HAS GAPS IN CONFORMING WITH THE FEDERAL INFORMATION TECHNOLOGY ACQUISITION REFORM ACT (FITARA)

Independent Auditor's Report

To: Office of Inspector General for the
U.S. Agency for International Development

This report presents the results of Brown & Company Certified Public Accountants and Management Consultants, PLLC's (Brown & Company) independent audit of the United States Agency for International Development's (USAID) implementation of the Federal Information Technology Acquisition Reform Act[1] (FITARA). The USAID Office of Inspector General (OIG) contracted with Brown & Company to conduct this independent audit of USAID's actions to establish a framework for management and oversight of its information technology (IT) assets, as prescribed by FITARA. This performance audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

Office of Management and Budget Memorandum (OMB) M-15-14, "Management and Oversight of Federal Information Technology," dated June 10, 2015, (OMB M-15-14) provides implementation guidance for FITARA and related IT management practices. It also establishes a Common Baseline[2] for roles, responsibilities, and authorities of the agency Chief Information Officer (CIO) and the roles and responsibilities of other applicable senior agency officials in managing IT as a strategic resource (henceforth referred to as "OMB M-15-14 Common Baseline").

USAID is a Chief Financial Officer (CFO) Act[3] agency required to implement FITARA. The OMB M-15-14 Common Baseline provides a framework for implementing the specific authorities that FITARA provides for CFO Act agency CIOs, and builds upon their responsibilities as outlined in the Clinger-Cohen Act of 1996.

The overall objective of this performance audit was to determine whether USAID established a framework for the management and oversight of its IT, as prescribed by FITARA. The secondary objective was to determine whether USAID established a comprehensive plan to implement Federal requirements for the management and oversight of its IT, as required by OMB M-15-14.

[1] Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. No. 113-291. Further references in the text that refer to "FITARA" refer to these sections.
[2] OMB M-15-14, "Attachment A: Common Baseline for IT Management and CIO Assignment Plan."
[3] Chief Financial Officers Act of 1990 (Public Law 101–576).

The scope of our audit included a review of USAID's FITARA Common Baseline Implementation Plan, USAID's IT strategic and operational plans, management policies, procedures, processes, practices for IT investments, and IT governance and control practices related to the implementation of FITARA. We obtained an understanding of the internal controls over the implementation of FITARA through interviews and observations, as well as inspections of various documents, including organizational policies and procedures. The audit fieldwork was performed at USAID's headquarters in Washington, D.C., from November 18, 2016, through December 13, 2017.

We concluded that USAID had not established a comprehensive framework to implement FITARA. Specifically, the Agency had not developed a comprehensive FITARA Implementation Plan that fully provides a framework for the management and oversight of its IT, as required by OMB M-15-14. We found that USAID had implemented only 7 of the 23 applicable requirements contained in OMB M-15-14 Common Baseline.[4] Consequently, the audit identified areas of improvement and included nine recommendations, which USAID should implement to conform to OMB M-15-14 Common Baseline requirements.

We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives. Our report contains the audit results and audit approach.

This report is for the purpose of concluding on the audit objectives described above. Accordingly, this report is not suitable for any other purpose.

We appreciate the assistance we received from the staff of USAID and appreciate the opportunity to serve you.

Sincerely,

Brown and Company
Largo, Maryland
October 17, 2018

[4] See detailed results for the 16 exceptions in Appendix II – OMB M-15-14 Common Baseline of this report.

1. INTRODUCTION

The United States Agency for International Development's (USAID) mission is to "partner to end extreme poverty and promote resilient, democratic societies while advancing its' security and prosperity." To accomplish its critical mission, USAID has relied increasingly on the use of information technology (IT). USAID's IT annual budget aligns resources to address USAID's IT strategic planning goals and multiple Presidential/Office of Management and Budget mandates. The Agency's IT budget enables USAID to enhance and strengthen mission-critical infrastructure; further develop a system to capture performance data; and support core acquisition-and-assistance and accounting systems.

Brown & Company Certified Public Accountants and Management Consultants, PLLC (Brown & Company) was engaged by USAID's Office of Inspector General (OIG) to conduct this audit to determine the extent to which USAID has implemented Federal Information Technology Acquisition Reform Act (FITARA)[5] requirements to improve IT management and oversight functions. To perform the audit, we used requirements contained in the Clinger-Cohen Act of 1996 (Clinger-Cohen Act), FITARA, and Office of Management and Budget Memorandum (OMB) M-15-14, "Management and Oversight of Federal Information Technology," (henceforth referred to as OMB M-15-14).

The Clinger-Cohen Act was enacted in 1996 to improve the acquisition and management of Federal IT resources. A key requirement of the Act called for the head of each agency to develop and implement a process for maximizing the value of IT acquisitions. The Act also established an approach for agencies to assess and manage IT acquisitions and risks to improve acquisition and oversight functions over IT resources by:

- Focusing information resource planning to support their strategic missions;
- Implementing a capital planning and investment control process that links to budget formulation and execution; and
- Rethinking and restructuring the way they do their work before investing in IT.

FITARA, enacted on December 19, 2014, augments the Clinger-Cohen Act's mandates by aiming to help increase transparency and visibility around IT spending and improve collaboration and information sharing between Federal entities. FITARA contains specific requirements related to:

- Agency Chief Information Officer (CIO) authority enhancements;
- Enhanced transparency and improved risk management in IT Investments;

[5] FITARA - Federal Information Technology Acquisition Reform Act. 12/19/2014. Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Public Law No: 113-291.

- Portfolio review;
- Federal Data Center Consolidation Initiative, which implements a data center consolidation inventory and optimization strategy;
- Expansion of IT acquisition training to Federal acquisition specialists and the use of IT skilled personnel in the acquisition of IT and IT related acquisitions;
- Maximizing the benefit of the Federal Strategic Sourcing Initiative, which provides guidance for the purchase of services and supplies; and
- Governmentwide Software Purchasing Program.

OMB M-15-14 states that all covered agencies [i.e., Chief Financial Officer (CFO) agencies] shall adopt specific controls for the management of IT from the "Common Baseline for IT Management," which covers the following sections: (1) budget formulation, (2) budget execution, (3) acquisition and (4) organization and workforce (henceforth referred to as "OMB M-15-14 Common Baseline"). In doing so, the Common Baseline provides a framework for CFO agencies to implement the specific authorities that FITARA provides for agency CIOs and builds upon their responsibilities as outlined in the Clinger-Cohen Act. As a CFO Act agency, USAID is required to implement FITARA.

2. BACKGROUND

FITARA, Public Law 113-291, was enacted on December 19, 2014. FITARA augments the Clinger-Cohen Act to address concerns about waste and ineffectiveness in Federal IT investments. FITARA seeks to combat waste and ineffectiveness through the implementation of a Common Baseline framework for IT management, applying economies of scale and implementation of best practices consistently across the Federal IT acquisition and management environment by:

- Re-emphasizing agency CIO authority and accountability over IT budget planning, formulation, execution, and protection to prevent the reassignment of IT funds to other programs;
- Empowering agency CIOs with new authority over hiring, project funding and approvals, and the delegation of responsibilities to sub-agency CIOs or CIO equivalents;
- Advocating agile/incremental development approaches for new systems to be used instead of traditional "specify in detail up front" approaches;
- Conducting annual reviews to reduce IT redundancies and improve costs, schedules, and outputs;
- Instituting governmentwide software purchasing to leverage centralized buying power and strategic sourcing;
- Centralizing authority over data center consolidation; and
- Developing an IT acquisition workforce with expanded access to specialized, highly skilled program and project managers.

OMB M-15-14 provides specific guidance and includes a Common Baseline of requirements to assist Federal agencies in consistently implementing FITARA. The requirements consist of 26 general requirements (23 are applicable to USAID) and

establish, among other things, minimum requirements for roles, responsibilities, and authorities of agency CIOs, as well as the roles and responsibilities of other applicable senior agency officials. Additionally, it requires Federal agencies to establish specific requirements in the following four areas: (1) budget formulation, (2) budget execution, (3) acquisition, and (4) organization and workforce. The guidance also requires agencies to perform an initial self-assessment to determine their current state in relation to the OMB M-15-14 Common Baseline requirements and to formulate an implementation plan to become compliant with those requirements. See Appendix II for descriptions of the OMB M-15-14 Common Baseline.

3. SUMMARY OF RESULTS

Our audit was performed in accordance with *Government Auditing Standards*, which require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We performed the audit fieldwork from November 18, 2016, through December 13, 2017.

The overall objective of this performance audit was to determine whether USAID established a framework for the management and oversight of its IT, as prescribed by FITARA. The secondary objective was to determine whether USAID established a comprehensive plan[6] to implement Federal requirements for its management and oversight of its IT, as required by OMB M-15-14. We conducted our audit by comparing the current state of USAID (i.e., its IT management and governance policies, practices, and procedures) and its FITARA Implementation Plan[7] to the OMB M-15-14 Common Baseline requirements to identify conformity or gaps in conformity.

We concluded that USAID had not established a comprehensive framework to implement FITARA. Specifically, the Agency had not developed a comprehensive FITARA Implementation Plan that fully provides a framework for the management and oversight of its IT, as required OMB M-15-14. We found that USAID had implemented 7 of the 23 applicable requirements contained in OMB M-15-14 Common Baseline.[8] However, its FITARA Implementation Plan did not fully address the remaining 16 requirements that the Agency had not implemented. These 16 gaps fall within eight findings. Specifically, the FITARA Implementation Plan did not fully address the need for:

1. The CIO to report directly to the Administrator, as required by OMB M-15-14 and the Clinger-Cohen Act.
2. USAID to adopt the FITARA definition for IT resources.
3. The CIO to have adequate oversight and decision authority over all budget execution activities related to the evaluation of IT resources, planned expenditures, and governance around IT policies and procedures.

[6] For this audit, a "comprehensive plan" is defined as a plan that, if implemented, will enable the Agency to meet requirements of the Federal Information Technology Acquisition Reform Act.
[7] USAID's FITARA Common Baseline Implementation Plan, v2 dated November 2015.
[8] See detailed results in Appendix II – OMB M-15-14 Common Baseline Requirements of this report.

4. The CIO to have authority to oversee IT resources across the entire Agency and its programs, and to have appropriate visibility and involvement in the management and oversight of IT resources.
5. USAID's policies and procedures to provide the CIO with the authorization to carry out oversight and decision authority over all USAID IT implementations to meet authorization to operate requirements.
6. The CIO to have authorization to enforce transparency for the IT inventory across the Agency.
7. USAID to maintain accurate records for managing the consolidation and streamlining of its IT resources and data centers.
8. The CIO and Chief Human Capital Officer (CHCO) to enforce the competency requirements for IT staff, including IT leadership positions.

We made nine recommendations to assist USAID in closing the above gaps. We acknowledge the Agency's management decisions on all recommendations. Based on our evaluation of the Agency's comments, we consider 3 recommendations closed, 5 recommendations resolved but open pending completion of planned activities, and 1 recommendation unresolved.

4. DETAILED FINDINGS

FINDING 1 – The FITARA Implementation Plan Did Not Fully Address the Need for the CIO to Report Directly to the Administrator as Required by OMB M-15-14 and the Clinger-Cohen Act.

OMB M-15-14, Attachment A, Sub-section Q1, "CIO reports to agency head (or deputy/Chief Operating Officer (COO))," states:

> 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."

Brown & Company inquired with USAID management, reviewed its organizational chart, and noted that the FITARA Implementation Plan did not fully address that the CIO did not report directly to the Administrator, as required by the OMB M-15-14 Common Baseline requirement and the Clinger-Cohen Act. Instead, the USAID organizational chart showed that the CIO has an indirect reporting relationship with the Deputy Administrator/Chief Operating Officer (COO). The CIO reported directly to the Assistant Administrator (AA) for the Bureau of Management (M). As a result, the CIO has limited authority in ensuring that IT issues and projects are funded and has been provided a priority level commensurate with the direction and goals of the Agency. For example, the CIO did not have adequate oversight and decision authority over all budget execution activities related to the evaluation of IT resources, planned expenditures, and governance around IT policies and procedures.

The current organizational reporting structure undermines the CIO's mandate to actively oversee and guide USAID's IT functions effectively, efficiently, and timely. Such a reporting structure may create delays in making critical IT and IT-related business decisions to align IT with USAID's strategic priorities. For example, as discussed in other findings in this report, the CIO did not have adequately assigned roles and responsibilities to meet FITARA's requirements.[9]

USAID OIG reported this weakness in Audit Report No. A-000-17-001-C, *USAID Has Implemented Controls in Support of FISMA*[10]*, but Improvements Are Needed,* dated October 27, 2016. In response to that report, USAID's former Deputy Administrator stated that:

> The agency is meeting the objectives of Clinger-Cohen and FITARA with the current reporting relationships and, therefore, no action is required on the recommendation. USAID has established management structures (e.g., the Management Operations Council) and other controls to ensure that the USAID CIO has direct access to the Administrator (or the Deputy acting on the Administrator's behalf) regarding IT programs and significant authority over the IT activities of the agency. In addition, the Office of the General Counsel advised that any requirement for a direct reporting relationship to the head of an agency can be delegated by the agency head, absent any statutory prohibition to such delegation. Clinger-Cohen and FITARA do not preclude such delegations.

USAID's AA/M subsequently submitted the following functional statement for the CIO to the Bureau for Management, Office of Management Policy, Budget, and Performance (M/MPBP) on October 27, 2017, to be incorporated in Automated Directives System (ADS) 101:

> The CIO reports directly to the Assistant Administrator, Bureau for Management, with respect to the day-to-day management of the Office of Chief Information Officer (M/CIO). The CIO has direct authority, and direct access to advise the Agency head, regarding whether to continue, modify, or terminate a program or project related to information technology (IT) and with respect to the acquisition of IT resources pursuant to provisions of the Paperwork Reduction Act (PRA), the Clinger-Cohen Act of 1996 (Clinger-Cohen) and FITARA.

However, the statement indicates that the CIO continues to have discretionary access to the Administrator or Deputy Administrator as opposed to a direct reporting relationship. Direct reporting, as required by the Clinger-Cohen Act, is more than discretionary linkage between the Administrator and CIO. It relates to direct supervision, which includes performance evaluations, goal setting, delegating, and task assignments. There is no direct reporting relationship when an official other than the Administrator is responsible for conducting the CIO's performance evaluation, and delegating and assigning tasks to the CIO.

[9] See Findings 3, 4, 5 and 6.
[10] Federal Information Security Modernization Act of 2014 (FISMA 2014).

In addition, OMB's position is that agencies with a statutory exception to Clinger-Cohen need not comply with Clinger-Cohen completely. Those agencies can get by with direct reporting to specified lower level officials if those agencies supplement this by allowing the CIO to have "direct access" to the agency head or deputy agency head. However, USAID's CIO does not report directly to the Agency head and the Agency does not have a statutory exception that allows the CIO to report to a lower-level Agency official.

Elevating the CIO's position to report directly to the Administrator, will increase the CIO's visibility and authority to effectively drive IT changes throughout USAID. It will also help the CIO successfully provide oversight of the IT portfolio as intended by FITARA.

RECOMMENDATION 1

We recommend that USAID's Administrator or Deputy Administrator develop and implement a governance structure so that the Chief Information Officer position reports directly to the Administrator, as required by the Federal Information Technology Acquisition Reform Act and the Clinger-Cohen Act of 1996.

FINDING 2 – The FITARA Implementation Plan Did Not Fully Address the Need for USAID to Adopt the FITARA Definition For IT Resources.

FITARA adopted the definitions of "IT" and "IT resources" found in the Clinger-Cohen Act of 1996, which requires all Federal agencies to adopt these definitions consistently. OMB M-15-14, Section A, "Defining the Scope of Resources Related to IT," also adopted the definitions of these terms with no change. It states that IT resources include all:

A. Agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation or other activity related to the IT lifecycle;
B. Acquisitions or interagency agreements that include IT and the services or equipment provided by such acquisitions or interagency agreements; but
C. Does not include grants to third parties that establish or support IT not operated directly by the Federal Government.

Further, that memorandum defines IT as:

A. Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that is/are used in the automatic acquisition, storage, analyses, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where
B. Such services or equipment are "used by an agency" if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the

services or equipment to a significant extent in the performance of a service or the furnishing of a product.

C. The term IT includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance); peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware, and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service); and related resources.
D. The term IT does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

Brown & Company reviewed USAID's definitions for IT and IT resources in the following policies and procedures:

- Automated Directives System (ADS) 301 "Responsibility for Procurement," dated August 31, 2011;
- ADS Glossary, dated April 30, 2014; Acquisition and Assistance Policy Directives (AAPD) 16-02 "Special Contract Requirements for Information Technology," dated May 3, 2016; and
- ADS 101 – Agency Programs and Functions, dated May 9, 2017.

Although the Agency had correctly defined IT, it had not correctly defined IT resources. Specifically, USAID's policies and procedures correctly defined IT as follows:

> Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes, but is not limited to, 'computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

However, the policies and procedures omitted definitions for IT resources to include budgetary resources, personnel, and facilities. The definition also omitted acquisitions and interagency agreements that include IT and the services or equipment provided by such acquisitions or interagency agreements.

Although the Agency's FITARA Implementation Plan states that the CIO will work to define the level of detail with which IT resources levels are described distinctly from other resources, the plan is not comprehensive. Specifically, due to an oversight, the plan did not include planned actions to adopt the FITARA definitions for IT resources.

The lack of full adoption of the FITARA definition of IT resources and the omission of certain IT resources resulted in the following weaknesses:

- Deficiencies in the implementation of IT, cybersecurity, and capital planning and investment controls, including the management and oversight of IT resources;

- Inaccurate CIO certification statements (IT resource statements) required by OMB Circular A-11;[11] and
- Inaccurate and incomplete Information Resources Management (IRM) Strategic Plans.

Failure to adopt the OMB M-15-14 definition could exclude some IT resources from being classified as IT assets, potentially causing USAID to be inconsistent with the governmentwide definition. By not being consistent with the governmentwide definition, the information may not be complete if, for example, OMB or other external parties try to determine the amount of IT across the Federal Government.

RECOMMENDATION 2

We recommend that USAID's Chief Information Officer revise the Agency's policy to adopt the definition of information technology resources and requirements presented within the Office of Management and Budget Memorandum M-15-14, "Management and Oversight of Federal Information Technology," including (1) information technology, budgetary resources, personnel, and facilities and publish that definition in the official USAID information technology policies, procedures and directives; and (2) acquisitions and interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements.

FINDING 3 – The FITARA Implementation Plan Did Not Fully Address the Need for the CIO to Have Adequate Oversight and Decision Authority Over All Budget Execution Activities Related to the Evaluation of IT Resources, Planned Expenditures, and Governance Around IT Policies and Procedures.

Public Law 113-291, Subtitle D (FITARA), 40 U.S.C. § 11319 (b)(1) states:

(A) The head of each covered agency … shall ensure that the CIO of the agency has a significant role in—(i) the decision processes for all annual and multi-year planning, programming, budgeting and execution decisions.
(B) (i) That the Chief Information Officer of each covered agency ... approve the information technology budget request of the covered agency.

OMB M-15-14, Attachment A, *Common Baseline for IT Management and CIO Assignment Plan* requires the following:

[11] OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," requires justification materials consisting of an analysis of resources and details resources associated with the actual program dollars going to IT investment, including an assurance statement by the agency CIO, consistent with FITARA and other relevant laws, affirming that the CIO has reviewed and approved the major IT investments portion of your budget request; a statement from the CFO and CIO affirming that the CIO had a significant role in reviewing planned IT support for major program objectives and significant increases and decreases in IT resources; and a statement from the CIO and CFO that the IT portfolio includes appropriate estimates of all IT resources included in the budget request.

- The CFO and CIO jointly define the level of detail with which IT resource levels are described distinctly from other resources throughout the planning, programming, and budgeting stages.
- CIO has a role in pre-budget submission for programs that include IT and [IT resources].
- CIO has a role in planning program management.
- CIO reviews and approves major IT investment portion of budget request.
- CIO defines IT processes and policies.
- CIO approval of reprogramming.

Brown & Company reviewed the Agency's policies and procedures for budget formulation, planning, and execution. The Agency's existing policies and procedures delegate the authority for the AA/M to administer a program of centralized support for the Agency's operations worldwide. However, these policies and procedures do not fully adopt specific controls for the management of IT from the "OMB M-15-14 Common Baseline for IT Management and CIO Assignment Plan" specified in FITARA.

For example, USAID did not demonstrate implementation of the CIO's role in the following budget elements identified in OMB M-15-14:

- Pre-budget submission for programs that include IT and IT resources;
- Planning program management; and
- Reviewing and approving of major IT investment portion of budget request.

In addition, the Agency did not demonstrate that the CIO was required to approve the reprograming or movement of funds for IT resources that required Congressional notification.

Brown & Company requested USAID's information system investment portfolio related to IT resources and budgeting, i.e., IT initiatives, projects, and ongoing acquired IT services. The submitted artifacts encompass the A-11 budget preparation requirements. However, USAID did not provide information about the actual budget formulation and execution. We also identified instances of budget execution decisions and use of IT resources by USAID operating units without the approval of the CIO.

Although, the FITARA Implementation Plan states that USAID will review the current budget development process and make changes to ensure involvement of the CIO, the plan is not comprehensive. Specifically, the plan did not specify, discuss, or define the level of authority, the role of the executives, or the process by which the program leadership will work with the CIO to plan an overall portfolio of IT resources. Therefore, the plan did not address the need for the CIO to have adequate oversight and decision authority over all budget execution activities related to the evaluation of IT resources, planned expenditures, and governance around IT policies and procedures. The FITARA Implementation Plan did not fully address these weaknesses because the CIO did not conduct detailed planning to implement FITARA.

The lack of the CIO's significant role in budget formulation, planning, execution of IT acquisitions, and the lack of properly defined roles and responsibilities for the CIO and CFO in the oversight of IT investments will prevent the USAID from meeting the FITARA requirements. In addition, this may prevent USAID from (1) achieving efficiency and effectiveness in IT investments; and (2) taking advantage of the economies of scale while leveraging USAID expertise when making specific mission and strategic IT investment and management decisions. It may also lead to waste, cost overruns in IT investments, and inefficiencies in the management of IT resources and issues in the CIO's certification statements (IT resource statements) as required by OMB Circular A-11.

In addition, the lack of policies and procedures that mandate that the CIO and program managers fulfill their shared and integrated responsibility increases the risk that legacy and ongoing IT investments will not be appropriately managed.

RECOMMENDATION 3

We recommend that USAID's Administrator or Deputy Administrator revise Automated Directives System 101 to provide the role, responsibilities, and authorities to the Chief Information Officer, as required by the Federal Information Technology Acquisition Reform Act, to oversee all annual and multiyear planning, programming, budgeting, and execution decisions, and reports related to information technology resources.

RECOMMENDATION 4

We recommend that USAID's Administrator develop and implement written policies that provide the Chief Information Officer with authorization to enforce the Federal Information Technology Acquisition Reform Act budget formulation and execution requirements by documenting the Chief Information Officer's oversight and decision authority, decision participation, and overall budget execution activities related to IT resources.

FINDING 4 – The FITARA Implementation Plan Did Not Fully Address the Need for the CIO to Have Authority to Oversee IT Resources Across the Entire Agency and its Programs, and to Have Appropriate Visibility and Involvement in the Management and Oversight of IT Resources.

OMB M-15-14, Attachment A, Sub-section E1, "Ongoing CIO engagement with program managers," states:

> The CIO should establish and maintain a process to regularly engage with
>
> program managers to evaluate IT resources supporting each agency strategic objective.

OMB M-15-14, Attachment A, Sub-section F1, "Visibility of IT planned expenditure reporting to CIO," states:

> The CFO, Chief Acquisition Officer, and CIO should define agency-wide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources.

OMB M-15-14, Attachment A, Sub-section I1, "Shared acquisition and procurement responsibilities," states:

> The CIO reviews all cost estimates of IT related costs and ensures all acquisition strategies and acquisition plans that include IT apply adequate incremental development principles.

Public Law 113-291, Subtitle D (FITARA), 40 U.S.C. § 11319(b)(1)(A), *Responsibility for Acquisitions of Information Technology, Resources, Planning, and Portfolio Management, 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 reports related to IT and the management, governance, and oversight processes related to IT.

Brown & Company reviewed USAID's policies and procedures related to its IT assets and investments that the Agency reported in production during fiscal years (FYs) 16–17. We selected three systems for testing: two (Abacus and DTRAMS) of 210 systems listed on the system inventory as of February 6, 2017, and Huddle. Also, we examined the CIO's accountability for centralized management and oversight, and centralized repository of information.

Of the three systems selected, the M/CIO could not provide the requested budget planning and execution documents for the first two aforementioned systems.

Further, the Agency lacked a detailed approach and plan of action to reconcile the number of IT assets and investments reported in production during FYs 16–17 and the number of IT assets and investments funded in FYs 16–17. The lack of such an approach is an indicator that the M/CIO has not developed and implemented a comprehensive centralized plan to implement FITARA.

The CIO also did not have adequate authority to oversee and review all IT investments and resources and related issues to prevent, detect, and correct shadow IT or hidden IT. Shadow IT or hidden IT refers to spending on IT that is not fully transparent to the Agency CIO and/or IT resources included as a portion of a program that is not primarily of an IT purpose but delivers IT capabilities or contains IT resources, e.g., a grants program that contains a portion of its spending on equipment, systems, or services that provide IT capabilities for administering or delivering the grants.

Although the FITARA Implementation Plan states that the current budget approval process will be revised to require that the CIO review and approve all major IT investments in the budget request, the plan is not comprehensive. Specifically, the plan did not define the changes that will be made in the approval process. Also, there is no discussion on how the CIO's approval or involvement will be communicated or documented.

The FITARA Implementation Plan did not fully address these weaknesses because the CIO did not conduct detailed planning to implement FITARA. Consequently, USAID has inefficiencies in the acquisition of IT resources and in the accuracy, and completeness of details reported to OMB due to:

- Challenges in managing a decentralized organization with more than 75 field missions and numerous field offices;
- The lack of a centralized approval process for the investments in IT resources; and
- The lack of a centralized repository to maintain details and documentation to comply with FITARA.

Congress should be able to monitor the Agency's progress and hold USAID accountable for reducing duplication and achieving cost savings in IT resources. However, the lack of a centralized approval process and repository limits the ability of the CIO to track, monitor, and ascertain whether each dollar spent maintains or enhances IT security posture and reduces risks.

RECOMMENDATION 5

We recommend that USAID's Chief Information Officer revise the existing policies and procedures to provide the Chief Information Officer with necessary oversight to maintain transparency of all information technology investments and acquisitions to prevent, detect, and correct shadow or hidden information technology.

FINDING 5 – The FITARA Implementation Plan Did Not Address the Need for USAID's Policies to Provide the CIO with the Authorization to Carry Out Oversight and Decision Authority Over All Agency IT Implementations to Meet Authorization to Operate Requirements.

OMB M-15-14, Attachment A, Sub-section J1, "CIO role in recommending modification, termination, or pause of IT projects or initiatives," states that the CIO may recommend to the agency head the modification, pause, or termination of any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation, within the terms of the relevant contracts and applicable regulations.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, CA-6 Security Authorization, states:

Control – The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

c. Updates the security authorization.

USAID's IT systems are required to obtain a signed ATO prior to implementation. Brown & Company selected the following systems to review their ATO documentation:

1. Abacus – (Office of U.S. Foreign Disaster Assistance (OFDA))
2. DTRAMS
3. Huddle

However, one (DTRAMS) of the three selected systems was in production without an ATO. Lack of the required ATO documentation indicates that the M/CIO was not able to carry out its ATO and continuous monitoring responsibilities, as required. This occurred because the Agency's policies and procedures did not provide the CIO with the authorization to carry out oversight and decision authority over all USAID IT implementations to meet ATO requirements in accordance with NIST.

According to Agency officials, DTRAMS was not provided an ATO because it is being decommissioned and replaced by UTRAMS, which is currently undergoing actions to obtain an ATO. However, those actions have not yet been completed.

Although the FITARA Implementation Plan states that the CIO will work to improve the process to make recommendations on the modification, termination, or pause on IT projects or initiatives including projects/initiatives within and outside of the CIO, the plan was not comprehensive. Specifically, the plan did not address the need for USAID's policies to provide the CIO with the authorization to carry out oversight and decision authority over all Agency IT implementations to meet authorization to operate requirements. Also, the plan did not define the areas of the process that require improvement, or how the process improvements will be implemented.

The FITARA Implementation Plan did not fully address these weaknesses because the CIO did not conduct detailed planning to implement FITARA. Consequently, the lack of a signed ATO reflects that the Agency has not complied with its system assessment and authorization process, and creates opportunities for IT security vulnerabilities to be introduced into the network.

RECOMMENDATION 6

We recommend that USAID's Chief Information Officer make written decisions whether to authorize DTRAMs, and take appropriate actions to comply with security assessment and authorization controls contained in National Institute of Standards and Technology Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations, CA-6 Security Authorization."

FINDING 6 – The FITARA Implementation Plan Did Not Address the Need for the CIO to Have Authorization to Enforce Transparency for the IT Inventory Across the Agency.

USAID must have an accurate and complete IT inventory in order for the CIO to fulfil his/her responsibilities under FITARA. As required by 40 U.S.C. § 11315 (c) (2):

> The CIO shall monitor the performance of information technology programs of the agency; evaluate the performance of those programs on the basis of the applicable performance measurements; and advise the head of the agency regarding whether to continue, modify, or terminate a program or project.

OMB Memo 15-14, Section JI, "CIO role in recommending modification, termination, or pause of IT projects or initiatives," states that the CIO role is responsible for recommending modification, termination, or pause of IT projects or initiatives. To fulfill this responsibility, the CIO must have an accurate and complete IT inventory.

Brown & Company reviewed the Agency's IT inventory reports and found that the CIO did not provide full transparency for IT inventory across the Agency. The system inventory is incomplete and does not support Senior Agency Officials (SAOs) with providing accountability and oversight of government-furnished equipment, and other hardware/software systems and assets that are connected to the network.

To illustrate, for FY16 USAID signed and issued 37 ATOs. However, USAID's Fiscal Year 2016 Fourth Quarter FISMA Report, Section 1A: Identify - System Inventory, showed that the IT inventory only contained 26 of the 37 inventory investments and assets. We requested, but did not receive, a detailed list/schedule of the 37 systems with ATOs and the 26 FISMA reportable systems.

Moreover, the number of IT investments reported on the IT Dashboard for Total FY16 Spending only included 23 IT investments. The auditors requested, but did not receive, a detailed list/schedule of the 23 IT investments.

IT assets in production in the USAID software development life cycle require CIO involvement in their budget formulation and execution. However, the CIO and staff cannot carry out their responsibilities under FITARA if the CIO and staff are not aware of and tracking the complete IT assets and investments inventories. Moreover, identifying all systems and assets would help SAOs facilitate management of cybersecurity risks to systems, assets, data, and capabilities.

The "Information Systems Decommissioning Plan" dated March 1, 2017, states:

> In order to support the decommissioning, USAID developed policies, such as Automated Directives System (ADS) Policy 577: Information Technology Capital Investment and Control (CPIC), which puts in place policy directives and procedures for controlling IT investments and assets. This policy enhances USAID investment control and management by:
>
> - Having a portfolio-focus, quantifying return on investment;

- Managing investment risk;
- Incorporating executive involvement; and
- Ensuring IT investments are architecture driven.

Through ADS 577, CPIC, and portfolio management processes, USAID is able to trace IT investments to specific information systems, and identify areas where cost efficiencies and savings can be achieved. The enactment and implementation of the Federal Information Technology Acquisition Reform Act (FITARA) will additionally enhance the responsibility and ability of M/CIO to monitor and control IT investments across USAID, and identify decommissioning candidates for information systems.

The above excerpt documents acknowledgement of the CIO's roles and responsibilities in managing IT systems inventory and the ability to crosswalk between IT investments, IT systems, and IT assets. However, there is a lack of properly defined roles and responsibilities for the CIO in inventory management and oversight of IT investments during the planning, programming, and budgeting stages. This caused a discrepancy between the inventory records of the number of IT assets actually funded, the number of IT investments reported, and the number of IT investments tracked in the USAID IT inventories.

However, the FITARA Implementation Plan did not fully address these weaknesses. The plan did not address these weaknesses because the CIO did not conduct detailed planning to implement FITARA. Consequently, the CIO could not accurately account for the procurement, budget formulation planning and execution, and risk for IT assets and investments and, therefore, could not accurately report to provide full transparency over IT acquisitions.

Further, the lack of a detailed approach and plan of action to account for the number of IT assets reported in production and the number of IT investments funded is an indicator that the M/CIO has not developed and implemented a comprehensive plan to implement FITARA.

RECOMMENDATION 7

We recommend that USAID's Chief Information Officer document and implement an inventory validation process to accurately and completely document information technology investments, information technology systems inventory, and Federal Information Security Modernization Act reportable systems inventory. That process must include providing the Chief Information Officer with oversight of information technology investments during the planning, programming, and budgeting stages of the system development life cycle, in accordance with Federal Information Technology Acquisition Reform Act.

FINDING 7 – The FITARA Implementation Plan Did Not Address the Need for USAID to Maintain Accurate Records for Managing the Consolidation and Streamlining of Its IT Resources and Data Centers.

OMB M-15-14, Attachment D: FY 2015 PortfolioStat describes changes to the PortfolioStat process, including reporting requirements for agencies. This attachment also describes the goals and topics that agencies and OMB needed to address through the PortfolioStat process. It states:

- **Commodity IT.** Agencies will discuss how they use category management to consolidate commodity IT assets; eliminate duplication between assets; and improve procurement and management of hardware, software, network, and telecommunications services. Furthermore, agencies will share lessons-learned related to commodity IT procurement policies and efforts to establish enterprise-wide inventories of related information.
- **Data Center, Cloud, and Shared Services Optimization.** Agencies will discuss their progress using cloud computing and shared services to optimize data center activities and achieve overall IT objectives. This includes a discussion of how the agency is using FedRAMP services and ensuring cloud services meet applicable FISMA requirements.

OMB M-15-14, Section D "Federal Data Center Consolidation Initiative (FDCCI)," states that (1) covered agencies shall prepare and provide to OMB comprehensive data center inventories; and (2) covered agencies shall provide multi-year strategies to consolidate and optimize data centers (Phase 1) and provide quarterly updates regarding phase one of FDCCI.

During Brown & Company's interviews and discussions with the M/CIO, the M/CIO team members could not describe and document how USAID uses category management to consolidate commodity IT assets; eliminate duplication between assets; and improve procurement and management of hardware, software, network, and telecommunications services. Furthermore, the CIO could not provide documentation of shared lessons-learned related to commodity IT procurement policies and efforts to establish enterprise-wide inventories of related information.

The M/CIO team members also could not provide a detail and accurate inventory of the Agency's data centers, IT investments and FISMA reportable systems. Further, the Agency's IT processes did not address maintaining accurate records for, and managing the consolidation and streamlining of its IT resources and data centers. Therefore, the CIO did not have processes and procedures to ensure the data related to IT resources and data centers were consolidated and streamlined.

Furthermore, the FITARA Implementation Plan did not assess category management and FDCCI requirements. Therefore, the plan did not address the above weakness.

Consequently, there is an increased risk that cloud services providers and IT data center services are not properly monitored. Also, USAID's assets are at risk of not being properly managed.

RECOMMENDATION 8

We recommend that the USAID's Chief Information Officer document and implement processes for maintaining accurate records for, and managing the consolidation and streamlining of, its information technology resources, systems, data centers, and other shared IT services in compliance with the OMB M-15-14.

FINDING 8 – The FITARA Implementation Plan Did Not Fully Address the Need for the CIO and Chief Human Capital Officer (CHCO) to Enforce the Competency Requirements for IT Staff, Including IT Leadership Positions.

As required by 40 U.S.C. § 11315(c)(3) *Agency Chief Information Officer* the CIO of an agency:

> (A) assesses the requirements established for agency personnel regarding knowledge and skills in information resources management and the adequacy of those requirements for facilitating the achievement of the performance goals established for information resources management.
>
> (B) assesses the extent to which the positions and personnel at the executive level of the agency and the positions and personnel at the management level of the agency below the executive level meet those requirements.

OMB M-15-14, Attachment A: *Baseline for IT Management, Critical Element and Control Activity*, P1 and P2, IT Workforce states:

> The CIO and CHCO will develop a set of competency requirements for IT staff, including IT leadership positions, and develop and maintain a current workforce planning process to ensure the department/agency can (a) anticipate and respond to changing mission requirements; (b) maintain workforce skills in a rapidly developing IT environment; and (c) recruit and retain the IT talent needed to accomplish the mission.
>
> CIO and CHCO—and CAO where relevant—shall develop a set of competency requirements for IT staff, including IT leadership positions, and develop and maintain a current workforce planning process to ensure the department/agency can (a) anticipate and respond to changing mission requirements; (b) maintain workforce skills in a rapidly developing IT environment; and (c) recruit and retain the IT talent needed to accomplish the mission.

USAID has not fully implemented OMB M-15-14, Attachment A: *Baseline for IT Management, Critical Element, and Control Activity*, P1 and P2, IT Workforce

Requirements. USAID is in the process of conducting competency assessments of IT specialists. However, the CIO lacks a current workforce planning process to ensure the Agency can (a) anticipate and respond to changing mission requirements; (b) maintain workforce skills in a rapidly developing IT environment; and (c) recruit and retain the IT talent needed to accomplish the mission.

The FITARA Implementation Plan did not address that USAID did not have an IT workforce strategy and that USAID has not defined the competency requirements for IT staff. Also, the plan did not include developing a process to enforce the competency requirements for the IT staff nor procedures for implementing the requirements. Furthermore, the plan did not fully address that the CIO and CHCO did not enforce the competency requirements for IT staff, including IT leadership positions.

The FITARA Implementation Plan did not fully address these weaknesses because the CIO did not conduct detailed planning for FITARA implementation. Consequently, without an IT workforce strategy, USAID faces the challenge of maintaining the right mix of IT employee skills, grades, and numbers to accomplish the mission in an effective and efficient manner.

RECOMMENDATION 9

We recommend that the USAID's Chief Information Officer, in coordination with the Chief Human Capital Officer, document and implement a process to enforce the competency requirements for information technology staff, including information technology leadership positions, and complete the assessment of competency requirements for information technology staff.

5. EVALUATION OF MANAGEMENT COMMENTS

On August 29, 2018, USAID provided its response to the draft report. The Agency's response is included in Appendix III.

The draft report included nine recommendations. Based on our evaluation of the Agency's comments, we consider:

- 3 recommendations closed (OIG recommendations 2, 7, and 8),
- 5 recommendations resolved, but open pending completion of planned activities (OIG recommendations 1, 3, 4, 5, and 9), and
- 1 recommendation unresolved (OIG recommendation 6).

Further, we acknowledge management decisions on all recommendations. Of those management decisions that we acknowledge, we disagree with the management decision on recommendation 6.

In response to OIG recommendation 1, USAID agreed with the recommendation. USAID revised the Agency's policies and procedures to state:

> The CIO has direct authority and direct access to advise the Agency head, regarding whether to continue, modify, or terminate a program or project related to … IT and with respect to the acquisition of IT resources pursuant to provisions of the Paperwork Reduction Act…, the Clinger-Cohen Act of 1996…, and FITARA.

USAID management also stated the following:

> As part of USAID's Transformation, the Agency is proposing a re-organized structure that draws a solid "direct" reporting line to the Administrator from the CIO and the CFO.

Further, USAID stated, after providing their written response, that the target transformation completion date is September 30, 2019, depending on Congressional approval of the USAID's reorganization proposal. Therefore, we acknowledge the Agency's management decision and, based on its planned actions, consider OIG recommendation 1 resolved but open pending completion of planned activities.

In response to OIG recommendation 8 (recommendation 2 in our report), USAID updated the Agency's policies and procedures to include the definitions of terms and requirements presented in OMB Memorandum M-15-14, including (1) information technology budgetary resources, personnel, and facilities and (2) acquisitions and interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements. Therefore, we acknowledge the Agency's management decision and, based on its actions, consider OIG recommendation 8 closed.

In response to OIG recommendation 2 (recommendation 3 in our report), USAID updated the Agency's policies and procedures to give the CIO the roles, responsibilities, and authorities, as recommended. For example, the policies and procedures state that the CIO:

- Oversees all Agency annual and multiyear planning, programming, budgeting, and execution decisions and reports related to information technology resources;
- Reviews and approves the Major IT Investment (as defined in OMB Memorandum M-15-14) portion of Agency budget requests, including providing the CIO affirmations in Agency budget justification materials required by FITARA; and
- Develops and implements Agency-wide policy for the level of detail all Bureau/Independent Offices (B/IOs) and the Agency must use to describe IT resource levels, distinct from other resources, throughout Agency planning, programming, budgeting, and reporting processes.

USAID's corrective action is consistent with the recommendation. Therefore, we acknowledge the Agency's management decision and, based on its actions, consider OIG recommendation 2 closed.

In response to OIG recommendation 3 (recommendation 4 in our report), USAID stated that they did not agree with the finding. Nonetheless, USAID updated the Agency's policies and procedures to document the CIO's authority for formulating and executing the information technology budget and overseeing information technology resources, as required by FITARA. However, the Agency did not provide documentation to demonstrate implementation of these policies and procedures. Therefore, we acknowledge the Agency's management decision and, based on its actions, consider OIG recommendation 3 resolved, but open pending completion of planned activities.

In response to OIG recommendation 4 (recommendation 5 in our report), USAID stated that they disagreed with findings because they felt that the auditors did not have a clear understanding of the relationship between IT Asset, IT Investment, IT Systems and FISMA Systems. The auditors explained that each category of IT assets has a life cycle that requires accountability and reconciliation. The majority of IT Investments for projects or initiatives will be IT assets and should be part of the annual asset inventory, as applicable.

USAID also stated that "a number of policies and processes are being updated and implemented to address the identified gaps in the area of expanding CIO oversight." USAID plans to complete this action by April 30, 2019. This plan of action will address the recommendation when it is completed. Therefore, we acknowledge the Agency's management decision and, based on its actions, consider OIG recommendation 4 resolved, but open pending completion of planned activities.

In response to OIG recommendation 5 (recommendation 6 in this report), USAID management did not agree with the finding. Their position is that "the requirement to carry out the oversight and decision authority, including issuing ATO, are all requirements of the Federal Information Security Modernization Act of 2014 (FISMA)

and not a part of the FITARA Common Baseline as defined in M-15-14." Also, the Agency expressed concerns about how the report referenced the FITARA Attachment D: FY15 PortfolioStat as criteria. However, we paraphrased the requirements under "Data Center, Cloud, and Shared Services Optimization" in OMB M-15-14. We determined that the FISMA criteria is appropriate for the implementation of FITARA because the Agency must ensure cloud services meet applicable FISMA requirements.

Also USAID management restated that "Abacus is part of OFDANet and, as such, is not considered a major application" and that "since OFDANet has an active Authorization to Operate (ATO), there is no need to issue a separate ATO to Abacus." We conducted additional research on the nature and content of information captured by Abacus in accordance with USAID's ADS 579, "USAID Development Data" (March 13, 2015). Based on our analysis, we agree with USAID's decision to include Abacus under the OFDANet ATO. As such, we removed from Finding 5 and recommendation 5 the narrative about Abacus needing an AT0. Therefore, USAID does not need to take additional action with respect to Abacus.

Also, in response to OIG recommendation 5, USAID stated that the M/CIO will evaluate the risks associated with DTRAMS and issue a written decision on whether to authorize DTRAMS to continue to operate while the replacement system, UTRAMS, is being developed and deployed. In their comments, USAID management stated that they planned to complete this action by August 31, 2018. This plan of action addresses the recommendation for DTRAM. Therefore, we acknowledge the Agency's management decision and consider OIG recommendation 5 resolved, but open pending completion of planned activities.

In response to OIG recommendation 6 (recommendation 7 in this report), USAID did not agree and stated that "there are already documented and implemented inventory validation processes that detail IT investments, IT systems, and FISMA-reportable systems. These processes are ongoing and continuously improving, but do exist, and therefore, USAID does not agree with the Recommendation." However, USAID was not able to demonstrate that they have an inventory validation process that traces IT investments to IT systems and FISMA-reportable systems. Therefore, we acknowledge the Agency's management decision, but disagree with it and consider OIG recommendation 6 unresolved.

In response to OIG recommendation 7 (recommendation 8 in this report), USAID stated that it disagrees with the finding. USAID agreed that the FITARA Common Baseline Implementation Plan did not address the need for managing the consolidation and streamlining of its IT resources and data centers, but stated that OMB M-15-14 did not call for it to be addressed.

In addition, USAID stated that it met the requirements to report its Data Center Inventory and that it follows the definition for data centers. USAID also mentioned holding quarterly meetings with OMB to discuss its inventory. However, these actions were not part of the finding. This finding is that the inventory information technology resources, systems, data centers, and other shared IT services were not accurate and could not be reconciled, and that this weakness should have been addressed in the FITARA implementation plan.

Nonetheless, the Agency provided evidence that accounted for its 84 non-tier data centers and demonstrated implementation of its process for maintaining accurate records which included its information technology resources, systems, data centers, and other shared IT services in compliance with the OMB M-15-14. Therefore, we acknowledge the Agency's management decision and consider OIG recommendation 7 closed.

In response to OIG recommendation 9, the Agency accepted the recommendation and has taken action to change its process to mandate that the IT workforce complete a competency assessment on an annual basis as part of the development of their Independent Learning and Training Plan. USAID's target completion date for this corrective action is January 31, 2019. Therefore, we acknowledge the Agency's management decision and based on its actions, consider OIG recommendation 9 resolved, but open pending completion of planned activities.

6. APPENDIX I – PURPOSE, OBJECTIVE, SCOPE AND METHODOLOGY

PURPOSE

USAID's Office of Inspector General engaged Brown & Company to evaluate USAID's implementation of FITARA.

OBJECTIVE

The overall objective of this performance audit was to determine whether USAID established a framework for management and oversight of its information technology as prescribed by FITARA. The secondary objective was to determine whether USAID established a comprehensive plan[12] to implement Federal requirements for its management and oversight of the USAID information technology, as required by OMB M-15-14.

SCOPE

The scope of our audit included a review of IT strategic and operational plans, management policies, procedures, processes, and practices for IT investments, and IT governance and control practices to determine whether USAID implemented the framework for management and oversight of its IT, as identified in OMB M-15-14.

Brown & Company reviewed policy documents, operating procedures available internally and publicly, and inquired with key management personnel to conduct the audit. The audit fieldwork was performed at USAID's headquarters in Washington, D.C., from November 18, 2016, through December 13, 2017.

METHODOLOGY

The methodology of this audit is based on *Government Auditing Standards* issued by the Comptroller General of the United States. Those standards require that Brown & Company plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the procedures used and the evidence obtained provides a reasonable basis for Brown & Company's findings and conclusions based on our audit objectives. The audit procedures included:

- Interviewing key personnel and reviewing policies and operating procedures to assess whether effective internal control over compliance with laws and regulations was maintained in all material respects, by
    - Gaining an understanding of internal control over compliance,
    - Evaluating management's assessment of internal control,

[12] For this audit, a "comprehensive plan" is defined as a plan that, if implemented, will enable the Agency to meet requirements of the Federal Information Technology Acquisition Reform Act.

  - Testing the design and operating effectiveness of internal control over compliance, and
  - Performing such other procedures, as we considered necessary to assess the existence and operating effectiveness of internal control in these circumstances.
- Interviewing key personnel with respect to IT management activities and related governance models;
- Reviewing key documents including the IT plans, committee structures, meeting minutes, relevant policies, and directives;
- Evaluating internal control over the implementation of FITARA to meet the audit objectives;
- Reporting the results and findings.

To test whether USAID implemented FITARA and OMB M-15-14 requirements in the management and oversight of its IT investments, Brown & Company judgmentally selected 2 of 210 systems in production (Abacus and DTRAMS) from the USAID system inventory list as of February 6, 2017, and the Huddle system for testing.

Since the samples selected were widely used application systems with significant investments, the test results had sufficient coverage to make a conclusion without the need for extrapolating the sample test results to the population. Because we used a judgmental sample, the results cannot be projected to the population.

Internal Control

As part of our audit, we considered internal controls that were significant to the audit objectives. The results of our audit include significant deficiencies in internal control over the implementation of FITARA. USAID did not fully implement 16 of the 23 applicable Common Baseline requirements.

Criteria

The criteria used for this audit include:

- Federal Information Technology Acquisition Reform Act, December 19, 2014.
- Office of Management and Budget Memorandum, M-15-14, “Management and Oversight of Federal Information Technology,” dated June 10, 2015.
- Clinger-Cohen Act of 1996.

7. APPENDIX II – OMB M-15-14 COMMON BASELINE REQUIREMENTS

Brown & Company compared USAID's actions to implement FITARA and its FITARA Implementation Plan against the applicable OMB M-15-14 Common Baseline requirements and identified the following gaps.

No.	Section	OMB M-15-14 Common Baseline For IT Management and CIO Assignment Plan	Audit Results
	A	**Defining the Scope of Resources Related to Information Technology**	
1		"Information technology resources" includes all: A. Agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology; B. Acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but C. Does not include grants to third parties, which establish or support information technology not operated directly by the Federal Government.	Identified Gap in Conformity; See Finding 2.
	B	**Implementation of the Common Baseline**	
2	**Subsection A**	**A1. Visibility of IT resource plans/decisions to CIO**. The CFO and CIO jointly shall define the level of detail with which IT resource levels are described distinctly from other resources throughout the planning, programming, and budgeting stages.	Identified Gap in Conformity; See Finding 3.
3	**Subsection B**	**B1. CIO role in pre-budget submission for programs that include IT and overall portfolio.** The agency head shall ensure the agency-wide budget development process includes the CFO, Chief Acquisitions Officer (CAO), and CIO in the planning, programming, and budgeting stages for programs that include IT resources (not just programs that are primarily IT oriented).	Identified Gap in Conformity; See Findings 3 and 4.

No.	Section	OMB M-15-14 Common Baseline For IT Management and CIO Assignment Plan	Audit Results
4	**Subsection C**	**C1. CIO role in planning program management.** The CIO shall be included in the internal planning processes for how the agency uses IT resources to achieve its objectives. The CIO shall approve the IT components of any plans, through a process defined by the agency head that balances IT investments with other uses of agency funding. This includes CIO involvement with planning for IT resources at all points in their lifecycle, including operations and disposition or migration.	Identified Gap in Conformity; See Findings 3 and 4.
5	**Subsection D**	**D1. CIO reviews and approves major IT investment portion of budget request.** CIO reviews and approves major IT investment portion of budget request. Agency budget justification materials in their initial budget submission to OMB shall include a statement that affirms: – the CIO has reviewed and approved the major IT investments portion of the budget request.	Identified Gap in Conformity; See Findings 3 and 4.
6	**Subsection E**	**E1. Ongoing CIO engagement with program managers.** The CIO should establish and maintain a process to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective.	Identified Gap in Conformity; See Findings 3 and 4.
7	**Subsection F**	**F1. Visibility of IT planned expenditure reporting to CIO.** The CIO of the agency has a significant role in the decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions.	Identified Gap in Conformity; See Findings 3 and 4.
8	**Subsection G**	**G1. CIO defines IT processes and policies.** The CIO defines the development processes, milestones, review gates, and the overall policies for all capital planning, enterprise architecture, and project management and reporting for IT resources.	Identified Gap in Conformity; See Finding 3.
9	**Subsection H**	**H1. CIO role on program governance boards.** The CIO shall be a member of governance boards that include IT resources.	Conforms.
10	**Subsection I**	**I1. Shared acquisition and procurement responsibilities.** The CIO reviews all cost estimates of IT related costs and ensures all acquisition strategies and acquisition plans that include IT, apply adequate incremental development principles.	Identified Gap in Conformity; See Findings 3 and 4.

No.	Section	OMB M-15-14 Common Baseline For IT Management and CIO Assignment Plan	Audit Results
11	**Subsection J**	**J1. CIO role in recommending modification, termination, or pause of IT projects or initiatives.** The CIO may recommend to the agency head the modification, pause, or termination of any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation, within the terms of the relevant contracts and applicable regulations.	Identified Gap in Conformity; See Finding 5.
12	**Subsection K**	**K1. CIO review and approval of acquisition strategy and acquisition plan**. Agencies shall not approve an acquisition strategy or acquisition plan (as described in FAR Part 724) or interagency agreement (such as those used to support purchases through another agency) that includes IT without review and approval by the agency CIO.	Identified Gap in Conformity; See Findings 3 and 4.
13	**Subsection L**	**L1. CIO approval of reprogramming.** The CIO must approve any movement of funds for IT resources that requires Congressional notification.	Identified Gap in Conformity; See Finding 3.
14	**Subsection M**	**M1. CIO approves bureau CIOs.** The CIO shall be involved in the recruitment and shall approve the selection of any new bureau CIO (includes bureau leadership with CIO duties but not title).	Not applicable to the business process.
15	**Subsection N**	**N1. CIO role in ongoing bureau CIOs' evaluations.** The Chief Human Capital Officer (CHCO) and CIO shall jointly establish an agency-wide critical element (or elements) included in all bureau CIOs' performance evaluations.	Not applicable to the business process.
16	**Subsection O**	**O1. Bureau IT Leadership Directory.** CIO and CHCO will conduct a survey of all bureau CIOs, and CIO and CHCO will jointly publish a dataset identifying all bureau officials with title of CIO or duties of a CIO.	Not applicable to the business process.
17	**Subsection P**	**P1. IT Workforce.** The CIO and CHCO will develop a set of competency requirements for IT staff, including IT leadership positions, and develop and maintain a current workforce planning process.	Identified Gap in Conformity; See Finding 8.
18	**Subsection Q**	**Q1. CIO reports to agency head (or deputy/COO).** 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."	Identified Gap in Conformity; See Finding 1.

No.	Section	OMB M-15-14 Common Baseline For IT Management and CIO Assignment Plan	Audit Results
	C	**Transparency, Risk Management, Portfolio Review, and Reporting**	
19	1	Standardized cost savings metrics and performance indicators. Part of the Integrated Data Collection (IDC) reporting requirements. Sharing with the public and Congress, as required by the Consolidated and Further Continuing Appropriations Act, 2015 (P.L. 113-235).	Conforms.
20	2	Monthly reporting. Covered agencies shall continue to provide updates of risks, performance metrics, project, and activity data for major IT investments to the Federal IT Dashboard (ITDB) as soon as the data becomes available, or at least once each calendar month. Data improvement program. If OMB or the agency CIO determines data reported to the ITDB is not timely and reliable, the CIO (in consultation with the agency head) must notify OMB through the IDC and establish within 30 days of this determination an improvement program to address the deficiencies.	Conforms.
21	3	Covered agencies shall hold PortfolioStat sessions on a quarterly basis with OMB, the agency CIO, and other attendees**.**	Conforms.
	D	**Federal Data Center Consolidation Initiative (FDCCI)**	
22	1	Covered agencies shall prepare and provide to OMB comprehensive data center inventories.	Identified Gap in Conformity; See Finding 7.
23	2	Covered agencies shall provide multi-year strategies to consolidate and optimize data centers (Phase 1) and provide quarterly updates regarding phase one of FDCCI.	Identified Gap in Conformity; See Finding 7.
	E	**Information Technology Acquisition Initiatives**	
24	1	IT Acquisition Cadres. FITARA's requirements for IT acquisition cadres builds upon OMB's Office of Federal Procurement Policy (OFPP) July 2011 memorandum on building	Conforms.

No.	Section	OMB M-15-14 Common Baseline For IT Management and CIO Assignment Plan	Audit Results
		specialized IT acquisition cadres. As originally required by the memorandum, *Acquisition Workforce Development Strategic Plan for Civilian Agencies - FY 2010 - 2014* of October 27, 2009, civilian CFO Act agencies shall continue to send their annual *Acquisition Human Capital Plans* to OMB OFPP.	
25	2	Category Management and the Federal Strategic Sourcing Initiative (FSSI). Agencies will be required to comply with an upcoming new rule regarding purchases of services and supplies of types offered under an FSSI agreement without using an FSSI agreement.	Conforms.
26	3	Governmentwide Software Purchasing Program and Category. The General Services Administration (GSA), in collaboration with OMB, shall create, and allow agencies access to, governmentwide enterprise software licenses through new awards as part of category management.	Conforms.

8. APPENDIX III – MANAGEMENT COMMENTS

The following is the full text of USAID's comments on the draft report, except we did not include the attachments provided.

MEMORANDUM TO THE ASSISTANT INSPECTOR GENERAL FOR AUDIT, THOMAS YATSCO

FROM: A-AA/M - Angelique M. Crumbly /s/
SUBJECT: Management Response to Draft Audit Report: *USAID has Gaps in Conforming with the Federal Information Technology Acquisition Reform Act* (Draft Audit Report No. A-000-18-XXX-C)

Thank you for the opportunity to review the draft report. The following are management's comments regarding the audit findings:

Recommendation 1: We recommend that USAID's Administrator or Deputy Administrator develop and implement a governance structure so that the Chief Information Officer position reports directly to the Administrator, as required by the Federal Information Technology Acquisition Reform Act and the Clinger-Cohen Act of 1996.

Management Decision: USAID concurs with the recommendation. USAID has taken further actions to clarify and implement the reporting relationship between the Administrator and the position of the Chief Information Officer (CIO). On April 25, 2018, in USAID General Notice 04183, the Agency announced revisions to ADS 101 *Agency Programs and Functions***(Tab 1)**. Section 101.3.1.6(b) includes a description of reporting relationships for the Chief Information Officer (CIO) that responds to the requirements of the Federal Information Technology Acquisition Reform Act (FITARA) and the Clinger-Cohen Act. The governance structure reflects a dual reporting arrangement for the USAID CIO and makes explicit the CIO's relationship to the USAID Administrator. This reporting structure empowers the CIO, at the CIO's discretion, to directly engage and advise the Administrator on Agency programs that include information technology (IT). It also enables the Assistant Administrator of the Bureau for Management to oversee, in a coordinated and integrated manner, the offices that provide administrative and operational support required for the effective and efficient delivery of Agency programs.

As described in ADS 101.3.1.6(b), the USAID CIO currently reports directly to the Assistant Administrator for Management (AA/M) for day-to-day general operations, and also has a reporting relationship to the USAID Administrator for all programs that include IT.

As part of USAID's Transformation, the Agency is proposing a re-organized structure that draws a solid "direct" reporting line to the Administrator from the CIO and the CFO. The proposed structure further elaborates the direct and indirect reporting relationships as requested by OMB. Specifically, that "the CIO position would still maintain both “direct” and “indirect” reporting requirements. The incumbent would directly report to the official supervisor of record, when determined by legislation, for purposes of decision making and overall job performance, which in this case, is the CIO reporting to the Administrator. To ensure closer alignment with other Agency central services, the CIO will also indirectly report to the AA/M who would provide daily guidance and coordination with other related M Bureau offices." This change in organizational reporting will directly address the OIG's reporting structure recommendations.

The Office of the CIO (M/CIO) would continue to be responsible for the oversight of the Agency’s IRM, as defined in the E-Government Act of 2002 and OMB Circular A-130; and the Agency’s IT resources, as defined in OMB Circular A-130 and FITARA; as well as for all CIO functions mandated by the Clinger-Cohen Act of 1996 and FITARA. The CIO in the proposed Bureau for Management would report directly to the Administrator, as OMB Circular M-15-14, the Clinger-Cohen Act of 1996 and FITARA specify, with daily management provided by the AA/M.

Target Completion Date: We request that this recommendation be closed upon issuance of the final audit report.

Recommendation 2: We recommend that USAID revise Automated Directives System (ADS) 101 to give the chief information officer the roles, responsibilities, and authorities to oversee all annual and multiyear planning, programming, budget execution decisions, and reports related to information technology resources, as required by the Federal Information Technology Acquisition Reform Act.

Management Decision: USAID concurs with the recommendation. A revision of ADS 101 was published on April 25, 2018 (**Tab 1**). Section 101.3.1.6(b) provided updates that included all of the roles, responsibilities and authorities cited in Recommendation 2.

Target Completion Date: We request that this recommendation be closed upon issuance of the final report.

Recommendation 3: We recommend that USAID develop and implement policies that give the Chief Information Officer authority for formulating and executing the information technology budget and overseeing information technology resources, as required by the Federal Information Technology Acquisition Reform Act.

Management Decision: USAID does not agree with Finding 3 of the Audit Report. Finding 3 states: *The FITARA Implementation Plan Did Not Fully Address the Need for the CIO to Have Adequate Oversight and Decision Authority Over All Budget Execution Activities Related to the Evaluation of IT Resources, Planned Expenditures, and Governance Around IT Policies and Procedures*. In fact, the USAID Federal Information Technology Acquisition Reform Act (FITARA) Common Baseline Implementation Plan of November 2015 (**Tab 2**), which was submitted to and approved by the Office of Management and Budget (OMB) in accordance with

M-15-14, specifically addresses the need for the CIO to have adequate oversight and decision authority over all budget execution activities related to the evaluation of IT resources, planned expenditures, and governance around IT policies and procedures. In addressing the sections A-D of the Common Baseline, the plan, on pages 8-12, specifically deals with the CIO role and authorities related to the: (A) Visibility of IT Resources; the (B) CIO role in pre-budget submission; the (C) CIO role in planning program management; and the (D) CIO role in budget requests. The Plan further detailed the actions that USAID proposed to take to address the identified gaps in each of these areas.

Along with other policy and process changes, a revision of ADS 101 was published on April 25, 2018 (**Tab 1**). Section 101.3.1.6(b) provided updates that give the Chief Information Officer authority for formulating and executing the information technology budget and overseeing information technology resources, as required by FITARA.

Target Completion Date: We request that this recommendation be closed upon issuance of the final audit report.

Recommendation 4: We recommend that USAID revise Agency policies and procedures to provide the Chief Information Officer with information needed for overseeing all information technology investments and acquisitions to prevent, detect, and correct shadow and hidden information technology.

Management Decision: USAID does not agree with Finding 4 of the Audit Report. Finding 4 states: *The FITARA Implementation Plan Did Not Fully Address the Need for the CIO to Have Authority to Oversee IT Resources Across the Entire Agency and its Programs, and to Have Appropriate Visibility and Involvement in the Management and Oversight of IT Resources.* In fact, the USAID FITARA Common Baseline Implementation Plan specifically addressed the gap that, "Currently the CIO lacks visibility into planned IT expenditures outside the CIO organization (pg. 14)." The Plan then specifically states the actions the Agency would take, led by the Chief Acquisition Officer (CAO), to address this gap (pgs. 14-15):

The CAO will review and revise the Agency acquisition policy to require the reporting to the CIO of all planned expenditures that include IT.

The CAO will work with other key stakeholders to define the level of detail required for the reporting of planned expenditures for all transactions that include IT resources.

USAID General Counsel (GC) will work with PPL, M/CIO, and other members of the USAID FITARA Working Group to update the Statutory Checklist addition to the Agency programming policy, to include FITARA and FISMA requirements.

The finding is further flawed in that it states:

Further, the Agency lacked a detailed approach and plan of action to reconcile the number of IT assets and investments reported in production during FYs 16–17 and the number of IT assets and investments funded in FYs 16–17. The lack of such an approach is an indicator that the M/CIO has not developed and implemented a comprehensive centralized plan to implement FITARA.

The statement and overall methodology demonstrates a lack of knowledge and understanding about how USAID and the Federal Government writ large operate. There is no need to reconcile the number of IT assets and investments since they are independent items with no direct correlation. This misunderstanding is also found in Finding 6 along with a number of other misunderstandings in the finding, which we have detailed below:

Brown & Company reviewed the Agency's IT inventory reports and found that the CIO did not provide full transparency for IT inventory across the Agency…

...To illustrate, for FY16 USAID signed and issued 37 ATOs. However, USAID's Fiscal Year 2016 Fourth Quarter FISMA Report, Section 1A: Identify - System Inventory, showed that the IT inventory only contained 26 of the 37 inventory investments and assets. We requested, but did not receive, a detailed list/schedule of the 37 systems with ATOs and the 26 FISMA reportable systems. Moreover, the number of IT investments reported on the IT Dashboard for Total FY16 Spending only included 23 IT investments. The auditors requested, but did not receive, a detailed list/schedule of the 23 IT investments.

This statement illustrates a misunderstanding of what constitutes a Federal IT system, a FISMA-reportable system, and an IT investment. There are no one-to-one relationships between these three items.

For example, USAID's M/CIO provides a list of FISMA Reportable Systems to the OIG on an annual basis as part of the Federal Information Security Management Act Audit (**Tabs 3, 4 and 5**).

More importantly, this statement illustrates the misunderstanding about the relationship between systems and IT investments. As part of the audit discussions in December 2017, M/CIO provided, "USAID's definitions, policies, and procedures for identifying IT Investments, IT Assets, IT Systems, FISMA Reportable Systems, and Investments to be reported on the IT Dashboard." These definitions (below) illustrate the difference in the items. For example, IT Investments do not equal IT systems or IT Assets as the auditors suggest, and therefore they cannot be reconciled.

IT Investments - Defined in Circular A-130: *z. 'Information technology investment' means an expenditure of information technology resources to address mission delivery and management support. This may include a project or projects for the development, modernization, enhancement, or maintenance of a single information technology asset or group of information technology assets with related functionality, and the subsequent operation of those assets in a production environment. These investments should have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment's most current alternatives analysis, if applicable.* (https://a130.cio.gov/definitions/)

IT Assets - Software, hardware or information system.

IT Systems - Per A-130: *w. 'Information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. § 3502).*

FISMA Reportable Systems – See "How Does M/CIO IA Determine FISMA Reportable Systems.pdf" (**Tab 6**)

Investments Reported on the IT Dashboard - In accordance with the previous administration's transparency initiatives, the Office of Management and Budget (OMB) launched a Federal Information Technology (IT) Dashboard. The IT Dashboard contains data received from agency *Exhibit 300* submissions, also known as the Major IT Investments. Non-IT Exhibit 300s (also IT investments) are not included on the IT Dashboard. The *Exhibit 300: Capital Asset Plan and Business Case Summary* supports the budget justification and reporting requirements for major information technology (IT) and non-IT investments as required by OMB Circular No. A-11 Part 7, Section 300: Planning, Budgeting, Acquisition, and Management of Capital Assets.

Also see page 40 of FY 2019 IT Budget - Capital Planning Guidance.

The draft audit report further states:

This caused a discrepancy between the inventory records of the number of IT assets actually funded, the number of IT investments reported, and the number of IT investments tracked in the USAID IT inventories.

The number of IT Investments has no correlation to the number of IT systems. IT Investments are discrete funding items that may or may not even correlate to a current IT system or could correlate to many IT systems. An IT Investment, for example, could be related to developing a new system and therefore would not be related to any existing system in the IT System Inventory. Other systems may be in Operations and Maintenance mode and require no investment at the time.

In following the plan of actions laid out in the USAID FITARA Common Baseline Implementation Plan, a number of policy and process updates were and are being implemented to address the identified gaps in the area of expanding CIO oversight. ADS 101.3.1.6(b) was revised to make explicit the role of the CIO in overseeing all Agency IT investment and acquisitions. In addition, to improve the visibility of IT resources to the CIO, USAID has revised the following Agency acquisition and programming policies: *ADS 300: Agency Acquisition and Assistance Planning* (**Tab 7**)*; Acquisition and Assistance Policy Directive 16-02* Revised (**Tab 8**); and *ADS 201: Program Cycle Operational Policy* (**Tab 9**)] and strengthened the IT investment governance process outlines in the Revised Charter for Information Technology Steering Subcommittee (**Tab 10**). These changes have improved the information available to the CIO for overseeing Agency information technology investments and acquisitions.

Finally, following its FITARA Implementation Plan, and in response to this recommendation, USAID will issue a new ADS chapter, ADS 509: *Management and Oversight of Agency Information Technology Resources*, a comprehensive Agency policy for the management and oversight of IT resources that will provide the CIO information needed for overseeing all IT

investments and acquisitions to prevent, detect, and correct shadow and hidden information technology.

Target Completion Date: April 30, 2019.

Recommendation 5: We recommend that USAID issue a written decision on whether to authorize Abacus (as a major application) and DTRAMS, and take appropriate actions to comply with security assessment and authorization controls in National Institute of Standards and Technology Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."

Management Decision: USAID does not agree with Finding 5 from the Audit Report. Finding 5 states: *The FITARA Implementation Plan Did Not Address the Need for USAID's Policies to Provide the CIO with the Authorization to Carry Out Oversight and Decision Authority Over All Agency IT Implementations to Meet Authorization to Operate Requirements*. While there is some truth to the fact that the USAID FITARA Implementation Plan did not address this need, the entire premise upon which it is based is faulty as the requirement to carry out the oversight and decision authority, including issuing Authorizations to Operate, are all requirements of the Federal Information Security Management Act (FISMA) and not a part of the FITARA Common Baseline as defined in M-15-14. The draft report incorrectly states that:

Per FITARA Attachment D: FY15 PortfolioStat process reporting requirements, agencies shall ensure IT acquisitions meet applicable FISMA requirements, such as Authorization to Operate (ATO) and subsequent continuous monitoring, in accordance with the National Institute of Standards and Technology (NIST) Risk Management Framework.

In fact, Attachment D states no such thing. The only reference in FITARA Attachment D (found here for easy reference https://management.cio.gov/implementation/) to FISMA is contained in the section re-printed below:

– **Data Center, Cloud, and Shared Services Optimization.** Agencies will discuss their progress using cloud computing and shared services to optimize data center activities and achieve overall IT objectives. This includes a discussion of how the agency is using FedRAMP services and ensuring cloud services meet applicable FISMA requirements.

Of the three systems the auditors requested to review; only one was a Cloud system subject to FedRAMP. This system, Huddle, was sponsored by USAID for FedRAMP authorization and remains a FedRAMP authorized system.

The Audit Report also states as part of Finding 5 that:

Specifically, the plan did not address the need for USAID's policies to provide the CIO with the authorization to carry out oversight and decision authority over all Agency IT implementations to meet authorization to operate requirements. Also, the plan did not define the areas of the process that require improvement, or how the process improvements will be implemented.

The FITARA Implementation Plan did not fully address these weaknesses because the

CIO did not conduct detailed planning to implement FITARA.

This is incorrect as the CIO conducted and continues to conduct very detailed planning regarding the implementation of FITARA, a comprehensive and complex law that requires policy, process, culture, and overall organizational change. This judgement statement is provided throughout the report with no evidence to support this assertion. The referenced plan did not address this authority because the CIO already had the authority to carry out oversight and decision making over all Agency IT implementations to meet authorization to operate requirements as part of FISMA.

The auditors recommend that the CIO exercise this very authority, which already exists, and issue authorization to operate for two non-cloud applications.

As was discussed at length with the auditors, Abacus is part of OFDANet and, as such, is not considered "a major application." Since OFDANet has an active authorization to operate (ATO), there is no need to issue a separate ATO to Abacus. USAID uses the definition of major applications as defined in *NIST Special Publication 800-18, Revision 1*.

In response to the recommendation, M/CIO will evaluate risks associated with DTRAMS and issue a written decision on whether to authorize DTRAMS to continue to operate while the replacement system, UTRAMS, is developed and deployed.

Target Completion Date: August 31, 2018.

Recommendation 6: We recommend that USAID document and implement an inventory validation process to accurately and completely document information technology investments, the information technology systems inventory, and the Federal Information Security Modernization Act reportable systems inventory.

Management Decision: USAID does not agree with Finding 6. Finding 6 states: *The FITARA Implementation Plan Did Not Address the Need for the CIO to Have Authorization to Enforce Transparency for the IT Inventory Across the Agency*. USAID does agree with the general statements in Finding 6 that, "*...the CIO role is responsible for recommending modification, termination, or pause of IT projects or initiatives. To fulfill this responsibility, the CIO must have an accurate and complete IT inventory*."

However, the FITARA Common Baseline Implementation Plan did not address the need for an IT inventory because it is not part of the Common Baseline in M-15-14.

Finding 6 continues the misunderstanding about the relationship between systems, FISMA Reportable systems and IT investments and uses it as justification for Recommendation 6.

There are already documented and implemented inventory validation processes that detail IT investments, IT systems, and FISMA-reportable systems. These processes are ongoing and continuously improving, but do exist, and therefore, USAID does not agree with Recommendation 6.

Since USAID has documented and implemented an inventory validation process to document information technology investments - ADS 577 Information Technology Capital Planning and Investment Control (**Tab 11**), including review and approval by the Investment Review Committee (**Tab 13**) and Information Technology Steering Subcommittee (**Tab 10**) followed by investment control through eCPIC and the Federal IT Dashboard, the information technology systems inventory Non-Compliant System ATO Plan (**Tab 14**), and the Federal Information Security Modernization Act reportable systems inventory (**Tabs 3, 4, 5 and 6**).

Target Completion Date: We request that this Recommendation be closed upon issuance of the final audit report.

Recommendation 7: We recommend that USAID document and implement processes for maintaining accurate records for, and managing the consolidation and streamlining of, its information technology resources, systems, data centers, and other shared information technology services in compliance with Office of Management and Budget Memorandum M-15-14.

Management Decision: USAID does not agree with Finding 7. Finding 7 states: *The FITARA implementation plan did not address the need for USAID to maintain accurate records for managing the consolidation and streamlining of its IT resources and data centers.* USAID agrees that the FITARA Common Baseline Implementation Plan did not address the need for managing the consolidation and streamlining of its IT resources and data centers because M-15-14 did not call for it to be addressed.

As the draft report points out, M-15-14 Attachment D calls for Fiscal Year 2015 PortfolioStat sessions, which are quarterly meetings held between USAID M/CIO staff and staff from the Office of Management and Budget, to include on the agenda "Commodity IT" and "Data Center, Cloud, and Shared Services Optimization." As directed, OMB placed these items on the Agenda and M/CIO regularly discusses these and the other topics from Attachment D with OMB. The draft report incorrectly uses M-15-14 Attachment D as evidence that USAID had a requirement it did not address.

Second, the draft report quotes M-15-14 Section D which refers to requirements around the Federal Data Center Consolidation Initiative (FDCCI). USAID met all of these requirements and still reports its Data Center Inventory to OMB on a quarterly basis (**Tab 15**).

Further, FDCCI was replaced in August 2016 by the Data Center Optimization Initiative via OMB Memorandum M-16-19 *Data Center Optimization Initiative*. USAID follows the definitions for data centers as defined in OMB M-16-19:

Data centers shall be categorized into two groups: tiered data centers and non-tiered data centers. Tiered data centers are defined as those that utilize each of the following: 1) a separate physical space for IT infrastructure; 2) an uninterruptible power supply; 3) a dedicated cooling system or zone; and 4) a backup power generator for prolonged power outages. All other data centers shall be considered non-tiered data centers.

Private sector-provided cloud services are not considered data centers for the purposes of this memorandum, but must continue to be included in agencies' quarterly inventory data submissions to OMB.

As such, USAID has no tiered data centers, 84 non-tier data centers and one "private sector-provided cloud service."

The draft report further states that M/CIO staff was unable to provide basic information that is regularly reported by USAID to OMB and OIG. For example, as mentioned, USAID reports its data center inventory on a quarterly basis, its IT investments regularly and publicly via the IT Dashboard and its FISMA reportable systems to OIG every year. USAID went through a data center consolidation and streamlining in 2012-2013 and, as noted above, now has no tiered data centers and only the one "private sector-provided cloud service." It seems that the auditor may have misunderstood that the single 'data center' (located at Terremark in Miami at the time) was the entire inventory.

Finally, USAID provided its Decommissioning Plan which is quoted in Finding 6. This plan describes the process for maintaining accurate records for and managing the consolidation and streamlining of USAID's IT resources, systems, data centers and other shared IT services. This is an ongoing enterprise architecture process.

USAID has documented and implemented a process for maintaining accurate records for, and managing the consolidation and streamlining of, its information technology resources, systems, data centers, and other shared information technology services. See Decommissioning Plan (**Tab 16**) and Decommissioning Quarterly Status Report (**Tab 17**).

Target Completion Date: We request that this Recommendation be closed upon issuance of the final audit report.

Recommendation 8: We recommend that USAID revise Agency policies, procedures, and directives to adopt the definitions of terms and requirements presented in Office of Management and Budget (OMB) Memorandum M-15-14, including (1) information technology budgetary resources, personnel, and facilities and (2) acquisitions and interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements.

Management Decision: USAID concurs with the recommendation. USAID updated the Glossary of ADS Terms on April 18, 2018, to include the definitions of terms and requirements presented in OMB Memorandum M-15-14, including (1) information technology budgetary resources, personnel, and facilities and (2) acquisitions and interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements. See *Glossary of ADS Terms,* partial revision dated 4/18/18, pgs. 133-135 (**Tab 18**). USAID also updated the following ADS Chapters to include the definition of terms and requirements on May 9, 2018 - see ADS Chapters 300 (**Tab 7**), 518, 519, 541-548, 552 and 577.

Target Completion Date: We request that this recommendation be closed upon issuance of the final audit report

Recommendation 9: We recommend that USAID document and implement a process to enforce the competency requirements for information technology staff, including those in information technology leadership positions, and complete the assessment of competency requirements for information technology staff.

Management Decision: USAID concurs with the recommendation. USAID has documented and implemented a process to enforce the competency requirements for information technology staff, including those in information technology leadership positions, and completed the assessment of competency requirements for information technology staff. The revision of ADS 101 (**Tab 1**) published on April 25, 2018, particularly Section 101.3.1.6(b) provided updates that included the following responsibilities:

Establishes, jointly with the Agency's Chief Human Capital Officer (CHCO), Agency-wide competency standards for all Agency IT staff, including IT leadership positions.

The Agency is additionally changing its process to mandate that the IT Workforce complete a competency assessment on an annual basis as part of the development of their Independent Learning and Training Plan (ILTP). A Standard Operating Procedure (SOP) for "Implementing and Enforcing Competency Requirements and Workforce Planning Process for USAID Information Technology Workforce" (**Tab 19**) is currently undergoing approval and will be implemented as part of the calendar year 2019 ILTP process.

Target Completion Date: January 31, 2019.