USAID
FROM THE AMERICAN PEOPLE

OFFICE OF INSPECTOR GENERAL

AUDIT OF USAID'S INFORMATION TECHNOLOGY GOVERNANCE OVER ITS PHOENIX OVERSEAS DEPLOYMENT AND PROCUREMENT SYSTEM IMPROVEMENT PROGRAM PROJECTS

AUDIT REPORT NO. A-000-06-001-P
February 21, 2006

WASHINGTON, DC

Office of Inspector General

February 21, 2006

MEMORANDUM

TO: Acting Chief Information Officer, John Streufert
Director Office of Acquisition and Assistance, Michael Walsh
Chief Financial Officer, Lisa D. Fiely
Director PPC/RA, Patricia Sommers
Director PPC/SPP, Roberta Mahoney

FROM: IG/A/ITSA Director, Melinda G. Dempsey /s/

SUBJECT: Audit of USAID's Information Technology Governance over Its Phoenix Overseas Deployment and Procurement System Improvement Program Projects (Report No. A-000-06-001-P)

This is our audit report on USAID's information technology governance over its Phoenix Overseas Deployment and Procurement System Improvement Program projects. In finalizing the report, we considered your comments on our draft report and have included them in their entirety as Appendix II.

This report contains six recommendations to help USAID improve its governance over Agency information technology initiatives. Based on your comments to our draft report, we consider that management decisions have been reached for Recommendation Nos. 1, 2, 3, 4, 5, and 6. For these recommendations, please notify the Bureau for Management's Audit, Performance and Compliance Division when final action is completed.

I want to express my sincere appreciation for the cooperation and courtesies extended to my staff during this audit.

U.S. Agency for International Development
1300 Pennsylvania Avenue, NW
Washington, DC 20523
www.usaid.gov

CONTENTS

SUMMARY OF RESULTS

The Information Technology and Special Audits Division of the Office of Inspector General in Washington, D.C. completed this audit to help the U.S. Agency for International Development (USAID) correct its long-standing material weakness in its information resources management processes. Specifically, this audit was initiated to determine whether USAID used Federal requirements and best practices to implement an integrated process to manage and control its Phoenix Overseas Deployment (POD) and Procurements System Improvement Program (PSIP) projects. (See page 3.)

USAID utilized some Federal requirements and best practices to implement an integrated process to manage and control its Phoenix Overseas Deployment and Procurement System Improvement Program projects, but did not implement several components of an effective information technology (IT) governance structure. Specifically, USAID did not:

- Update its information resources management strategic plan.
- Fully develop an Agency Enterprise Architecture.
- Prepare, complete, and/or codify some policy and procedures for its IT processes.
- Fully establish its Program Management Office. (See pages 5-12.)

These weaknesses occurred primarily because USAID did not provide its' Chief Information Officer with control to ensure sufficient resources were available for an effective IT governance structure. As a result of the weaknesses, USAID did not always use its IT resources responsibly and manage its IT risks appropriately. Specifically, USAID was unsuccessful with its PSIP project and had some undisciplined practices that led to deficiencies in its POD project. Moreover, USAID may continue to:

- Have difficulty aligning its IT with the business.
- Develop its systems in a "stovepipe" manner.
- Be unable to repeat its successes and thus maximize IT resources. (See pages 12-20.)

As such, we are making six recommendations to help USAID improve its IT governance over Agency IT initiatives. (See pages 7, 9, 10, 12, and 13.) Although USAID management disagreed with some statements made in the report, they agreed to take corrective actions to implement all of the recommendations. (See pages 21-25.)

BACKGROUND

The Clinger-Cohen Act of 1996 requires the heads of executive agencies to implement a process that maximizes the value and assesses and manages the risks involved in information technology (IT) investments. The process is to include, among other things:

- Procedures to select, manage, and evaluate investments.
- A means for senior managers to monitor progress in terms of costs, system capabilities, timeliness, and quality.

IT governance provides the structure that links IT processes, resources and information to enterprise strategies and objectives. The objectives are to (1) align IT with the business, enable the business and maximize resources; (2) use IT resources responsibly; and (3) appropriately manage IT risks. IT governance is especially important in an environment where the Chief Information Officer has limited funds. Some of the key components of an IT governance structure are:

- An information resources management strategic plan, which provides a description of how information resources management activities help accomplish agency missions.
- An enterprise architecture, which is a description and documentation of the current and desired relationships among business and management processes and IT.
- IT policies and procedures.
- IT organizational structure.
- Controls to manage the project, its associated risks, and the quality of deliverables.

According to USAID's fiscal year 2004 "Performance and Accountability Report," USAID has taken steps to meet the goals of its business transformation—a multi-year, multi-step plan to reform the Agency's management systems and improve organizational performance. One component of USAID's transformation initiative is the Agency's Business Systems Modernization plan to establish a worldwide business platform capable of supporting higher levels of performance. The plan's overall goal is to enhance the delivery of Agency services and programs through Internet-enabled, globally deployed systems and standardized processes and practices.

Two key IT initiatives under the Business Systems Modernization plan are:

- Phoenix Overseas Deployment Project - In an effort to correct a longstanding material weakness with its accounting system, USAID is deploying its core accounting system (called Phoenix) to its overseas Controller missions. In August 2004, USAID put the system into production at five pilot missions. Subsequently, USAID went live with Phoenix in its missions in (1) Latin American and Caribbean and (2) Europe and Eurasia regions in February 2005 and July 2005, respectively. Over the next year, USAID plans to deploy the system to

its missions in the remaining two regions, (1) Africa and (2) Asia and the Near East. USAID's estimate of the cost to implement the system is $26.5 million.[1]

- Procurement System Improvement Program (PSIP) – In August 2004, USAID began its PSIP project to improve the efficiency and effectiveness of acquisition and assistance processes throughout the Agency. Specifically, the project is designed to (1) replace the New Management System legacy system for Acquisition and Assistance, which is used only in USAID/Washington, and (2) automate the paper process at USAID missions—which initiate more than half of the Agency's procurement transactions. To accomplish such improvements, USAID planned to implement a commercial off-the-shelf solution at a cost of approximately $26.8 million.

Since 1997, USAID has reported a material weakness[2] in its information resources management processes. The key weakness was that USAID's IT programs lacked sufficient safeguards against waste and mismanagement, as demonstrated by the (then) over-budget, unsuccessful attempt to rollout the Agency's new management information systems. Specifically, the Agency did not have a:

- Strategically oriented IT capital investment planning, budgeting, and acquisition process.

- Tactically oriented IT investment program management control capacity.

In November 2004, USAID reported that closure of the material weakness was contingent upon the full implementation of tactically oriented program management and oversight practices. Further, USAID would demonstrate that such practices were effective by completing the implementation of a project, which was expected by the end of fiscal year 2005.

AUDIT OBJECTIVE

This audit was initiated to help USAID correct its material weakness in its information resources management processes. As such, this audit was added to the Office of Inspector General's annual audit plan to answer the following question:

> Did USAID utilize Federal requirements and best practices to implement an integrated process to manage and control its Phoenix Overseas Deployment and Procurement System Improvement Program projects?

Appendix I contains a discussion of the audit's scope and methodology.

[1] Subsequent to our audit fieldwork, USAID deployed Phoenix in its ANE missions on December 13, 2006.

[2] This material weakness is reported pursuant to the Federal Managers' Financial Integrity Act.

AUDIT FINDINGS

USAID utilized some Federal requirements and best practices to implement an integrated process to manage and control its Phoenix Overseas Deployment (POD) and Procurement System Improvement Program projects (PSIP), but did not implement several components of an effective information technology (IT) governance structure.

For example, USAID utilized the following Federal requirements and best practices to manage and control its projects:

- Increased the staffing of its Program Management Office (PMO).
- Appointed Directors for its Office of Information Resources Management and PMO.
- Established a Business Transformation Executive Committee to provide Agency-wide leadership for initiatives and investments to transform USAID business systems and organizational performance.

In addition, USAID created some resources for Agency IT initiatives. For example, it:

- Published its "Risk Management Plan," which provides a framework for teams to take appropriate measures to minimize adverse impacts to scope, cost, and schedule.
- Published a "Quality Control Plan," which, according to the document, establishes quality control for Business Transformation projects through the application of planning, monitoring, deliverable review, and reporting activities.
- Substantially revised its policy directives for planning, budgeting, and managing USAID's capital IT assets, which, among other requirements, added a quarterly review process for IT investments.
- Drafted an Automated Directives System chapter that addresses earned value management, a technique that provides project managers and others visibility into the technical, cost, and schedule progress of their projects and contracts.

Nonetheless, USAID did not implement several components of an effective IT governance structure. Specifically, USAID did not (1) update its information resources management (IRM) strategic plan, (2) fully develop an Agency enterprise architecture (EA), (3) prepare, complete, and/or codify some policy and procedures for its IT processes, and (4) fully establish its PMO. In the finding (below), the first major section "Several Key Components of an Effective IT Governance Structure Needed" (pages 5-12) discusses these problem areas. The second major section, "CIO Not Provided Control To Ensure Sufficient Resources for an Effective IT Governance Structure" (pages 12-14) discusses the causes of the problem areas. The third major section, "IT Resources Not Always Used Responsibly and IT Risks Not Always Managed Appropriately" (pages 14-20) discusses the impact of the problem areas.

USAID Did Not Implement Several Key Components of an Effective IT Governance Structure

Summary: USAID did not implement several key components of an effective IT governance structure, as required by Federal requirements and best practices. Specifically, USAID did not (1) update its IRM strategic plan, (2) fully develop an Agency EA, (3) prepare, complete, and/or codify some policy and procedures for its IT processes, and (4) fully establish its PMO. These weaknesses occurred primarily because USAID's CIO was not provided control to ensure sufficient resources for an effective IT governance structure. As a result, USAID did not always use its IT resources responsibly and manage its IT risks appropriately. Specifically, USAID was unsuccessful with its PSIP project and used some undisciplined practices that led to deficiencies in its POD project. Moreover, USAID may continue to (1) have difficulty aligning its IT with the business, (2) develop its systems in a "stovepipe" manner, and (3) be unable to repeat its successes and thus maximize IT resources. The following paragraphs discuss this issue in detail.

Several Key Components of an Effective IT Governance Structure Needed – As discussed below, USAID did not implement several key components of an effective IT governance structure.

IRM Strategic Plan Outdated - Office of Management and Budget (OMB) Circular No. A-130, "Management of Federal Information Resources," establishes policy for the management of Federal information resources. The Circular states that, in the capital planning and investment control process, agencies must prepare an IRM plan that is strategic in nature and addresses all aspects of information resources management of the agency. IRM Strategic Plans should support the agency Strategic Plan; provide a description of how information resources management activities help accomplish agency missions; and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

Further, Automated Directives System (ADS) 542, "Planning and Budgeting for IT Resources," provides a framework and the essential procedures for planning and budgeting for information management and IT resources to carry out the Agency's mission, goals, and objectives. Section 542.5.2 requires that USAID develop an Agency-wide IRM Strategic Plan for the creation, collection, processing, transmission, use, storage, dissemination, and disposition of information. It also states that the IRM strategic planning process shall support the Agency's current and future mission and program needs, and include participation from the Agency's bureaus, independent offices, and missions. The ADS further states that the IRM Strategic Plan shall serve as the cornerstone for formulating the Agency-wide IRM budget submission to OMB. Finally, section E542.5.2 requires that the IRM Strategic Plan be updated annually.

In February 2005, the Office of Inspector General reported that USAID had not updated its plan since 2000.[3] For this reason, the audit recommended that USAID's Chief Information Officer update the IRM plan to address the Agency's information technology requirements, priorities, and infrastructure challenges over the next five years. In response to the audit report, USAID's Chief Information Officer agreed to revise the plan. To accomplish this, USAID tasked a contractor to incorporate USAID's unique business requirements into the 2006-2010 plan. Because USAID is continuing to update its IRM strategic plan, we are not making a recommendation at this time.

EA Not Fully Developed – According to OMB A-130, an agency's capital planning and investment controls process must build from the agency's current EA. An EA is defined as "the explicit description and documentation of the current and desired relationships among business and management processes and information technology." The EA includes:

- The rules, standards, and life-cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio.

- A strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment.

- Principles and goals to set direction in the areas of promoting interoperability open systems, public access, end-user satisfaction, and IT security.

To create and maintain an EA, agencies must have a framework to document linkages between mission needs, information content, and information technology capabilities. This framework will guide both strategic and operational IRM planning. Once the framework is established, the agency must create the EA.

USAID adopted the CIO Council's "Federal Enterprise Architecture Framework" (September 1999) as its EA framework. The Federal EA framework defines five major components that are needed to develop an EA:

- A data reference model, which promotes the common identification, use, and appropriate sharing of data/information.

- A business reference model, which describes the Federal government's line of business in an effort to promote agency collaboration.

- A technical reference model, which provides a foundation to describe the standards, specifications, and technologies supporting the secure delivery, exchange, and construction of business components and e-Gov solutions.

- A service component reference model, which classifies service components with respect to how they support business and/or performance objectives.

[3] Audit Report No. A-000-05-006-P, "Audit of USAID's Information Technology Infrastructure," February 22, 2005

- A performance reference model, which provides a suggested process to develop IT performance information that can be used to improve decision-making and performance.

In March 2004, USAID completed its EA (both current and desired) for the Agency's HIV/AIDS Programs. According to USAID officials, some of the lessons learned from that EA will be applied to the Agency-wide EA. Using OMB's "Guidelines for Enterprise Architecture Assessment Framework," (April 2004), USAID officials self-assessed the EA for the HIV/AIDS program at 3.94 out of 5 possible points.[4]

To date, USAID has developed the current (or as-is) EA for the business, technical, service component, and performance reference models. However, USAID has not yet developed a current EA for the data reference model—a critical component—which identifies the manner in which data are organized and integrated. Moreover, USAID has not yet developed the desired (or "to be") EA. As such, USAID has not integrated its business process and information in a holistic way to guarantee an alignment of business and technology. Therefore, we are making the following recommendation.

Recommendation No. 1: We recommend that the Chief of the USAID Program Management Office's Business Enterprise Architecture Division develop and implement a plan to address the enterprise architecture needs of the Agency.

Evaluation of Management Comments - In response to the draft audit report, USAID management noted that the Joint Enterprise Architecture is currently managed by the Department of State. Based on Agency's comments and further discussions, we modified our recommendation that USAID complete the development of its current and desired enterprise architecture, in accordance with Office of Management and Budget Circular No. A-130. Nevertheless, USAID management agreed to develop a project plan that will address USAID's enterprise architecture objectives. For the Executive Information System, USAID management agreed to develop a data reference model focusing on the data that supports the program and activities management. Further, USAID management stated that other elements of the model will be developed as budget and management priorities permit. Based on the above, we consider that a management decision has been reached for Recommendation No. 1.

Many Policies[5] and Procedures[6] Non-Existent, Fragmented, and/or Not Codified in ADS – According to the ADS 101, "Agency Programs and Functions," the PMO's Enabling Technologies and Integration Division's responsibilities include establishing and maintaining Agency policies, processes, and procedures regarding the information technology life cycle, systems engineering, program management, methods and activities.

USAID's PMO created the online Project Management Guidebook (the Guidebook) to provide IT managers with a standardized approach to managing IT projects. The Guidebook states that its guidelines are consistent with best practices from the Project

[4] Unaudited
[5] Policies are clear and concise rules and regulations necessary for the conduct of Agency business.
[6] Procedures are detailed courses of action that must be followed.

Management Institute and Software Engineering Institute.[7] The Guidebook identifies phases for each IT project, which consist of a series of required and discretionary activities.

While the Guidebook is a beginning, as discussed below, more work is needed as many policies and procedures were non-existent, fragmented, and/or not codified in the ADS, USAID's official Agency-level policies and procedures.

Many Policies and Procedures Non-Existent – The Guidebook identifies ADS Chapter 577, "Information Technology Capital Planning and Investment Control" as the Agency's policy and procedures for most activities of one project phase.

However, USAID did not establish policies and procedures for any of the other nine project phases or the corresponding activities. For example, USAID did not develop policies and procedures for:

- Developing user requirements.
- Handling users' qualified acceptance of a new system (e.g., either fully address user concerns before moving forward or obtain a waiver).
- Completing operational readiness reviews when deploying a system.
- Performing tests of software before it can be selected and procured.
- Conducting independent verification and validation as a standard part of project development based on, for example, dollar or project impact thresholds.

In addition, although the Guidebook states that many of the activities are discretionary depending on the system and may be abbreviated or merged with other documents and/or activities, USAID did not establish policies and procedures for determining when those activities should be performed. For example, USAID did not establish what factors (e.g., risk of investment, dollar threshold, or impact of the system on the Agency as a whole) must be considered when determining whether the discretionary activities should be performed.

Finally, USAID did not establish policies and procedures to identify the required inputs or outputs (e.g., plans, decision points, and reports) to move to the next phase of the project.

Similarly, an April 2005 study[8] performed on USAID's behalf states that many of the ADS documents were developed "…without a common, or centralized, management approach to IT governance and only tangentially address some of the elements of IT governance…." Therefore, we are making the following recommendation.

[7] The Software Engineering Institute is a part of Carnegie Mellon University.
[8] "USAID IT Governance: Current Structure," April 2005

Recommendation No. 2: We recommend that the Chief of the USAID Program Management Office's Enabling Technologies and Integration Division develop USAID's policies and procedures for each phase and activity of the Agency's project life cycle, including performance metrics and measures.

Evaluation of Management Comments - In response to the draft audit report, USAID management agreed to coordinate the development of USAID's IT Project Management Control Manual (the manual) which will describe the the policies and procedures for each phase and activity of the Agency's information technology (IT) project life cycle. The manual will be a mandatory reference to the Automated Directive System (ADS). Based on the above, we consider that a management decision has been reached for Recommendation No. 2.

Some Polices and Procedures Fragmented – According to the Government Accountability Office's *Standards of Internal Controls in the Federal Government*, all significant events need to be clearly documented, and the documentation should be readily available for examination. However, although USAID developed ADS 577, "Information Technology Capital Planning and Investment Control," that directive does not provide policy and procedures for validating and maintaining the support for cost information in the OMB 300s. OMB 300s are designed to (among other things) present the business case for making the investment, including cost, schedule, and performance goals for the investment.

Validating and maintaining the support for cost information is necessary because cost estimates undergo numerous iterations during their life cycle. According to USAID officials, the estimates often start as a white-boarding exercise that gets firmed up using the collective knowledge base of all of the participants. This cycle is repeated as often as necessary. Next, USAID and the OMB adjust the estimates during the normal review process. Due to these necessary but complex procedures, it is difficult to trace the final estimates with the business decision that created them, unless supporting documentation is maintained. As a result, decision-makers make capital investment decisions without the ability to validate the costs of individual components and the costs associated with each budget year. Therefore, we are making the following recommendation.

Recommendation No. 3: We recommend that the Chief of USAID Program Management Office's Enabling Technologies and Integration Division prepare Agency policies and procedures for preparing Office of Management and Budget Exhibit 300s to require that documentation be maintained for cost estimates and that the cost estimates be validated.

Evaluation of Management Comments - In response to the draft audit report, USAID management agreed to develop guidance for preparing IT system life cycle cost estimates and their validation. This guidance will be a mandatory reference to the ADS. In addition, the earned value managent procedures (developed in response to recommendation 4) will include a requirement for the validation of major investment performance baselines. Based on the above, we consider that a management decision has been reached for Recommendation No. 3.

Some Policies and Procedures Not Codified in ADS – According to ADS 501, "The Automated Directives System," section 501.3.1, all Agency-level internally created policy directives and required procedures must be codified in the ADS. However, although USAID developed some standards that should be followed for IT projects and made those standards available on the PMO website, policies and procedures for following those standards have not been incorporated into the ADS. Such examples include the risk management plan and the quality control plan, as described below.

- Risk Management Plan – According to the PMO's risk management plan, it provides (1) a framework for teams to take appropriate measures to minimize adverse impacts to scope, cost, and schedule; and (2) USAID Executive Sponsors, Business Transformation Project Managers, and Governance Bodies with processes and information to make decisions regarding project and program alternatives. Although that document is available on the PMO's website, a requirement to follow it has not been incorporated into USAID's Automated Directives System.

- Quality Control Plan – According to the PMO's Quality Control Plan, it establishes the policy for quality control for Business Transformation projects through the application of planning, monitoring, deliverable review, and reporting activities. Although that document is available on the PMO's website, a requirement to follow it has not been incorporated into USAID's Automated Directives System.

Therefore, we are making the following recommendation.

> *Recommendation No. 4: We recommend that the Chief of the USAID Program Management Office's Enabling Technologies and Integration Division codify USAID's policies and procedures for project risk management, quality control, and earned value management in accordance with USAID's Automated Directives System Chapter 501.*

Evaluation of Management Comments - In response to the draft audit report, USAID management agreed to develop and codify project policies and procedures for project risk management, quality control, and earned value management. Based on the above, we consider that a management decision has been reached for Recommendation No. 4.

PMO Evolving and Not Fully Established – In a March 1999 audit,[9] the OIG reported that USAID continued to manage its modernization through committees rather than by adopting the recommended program management approach. As a result, USAID's risk that the modernization efforts would encounter delays and cost increases and that the new system would not operate effectively when deployed increased significantly. To correct the weakness, the audit report recommended that USAID's Chief Information Officer work collaboratively to establish a strong program management office or function, with sufficient responsibility, authority, and resources to apply disciplined practices to implement financial management system improvements.

[9] Audit Report No. A-000-99-003-P, "Audit of USAID's Progress Implementing a Financial Management System That Meets Federal Financial Management Improvement Act Requirements," March 1, 1999.

Therefore, USAID's Business Transformation Executive Committee established the PMO to (1) improve and standardize project management practices used by Agency project teams and (2) provide assistance to Business System Modernization and other projects. The overall goal of the PMO is to accelerate delivery of business benefits from investments by using proven tools, processes and knowledge to meet project scope, quality, schedule, and cost expectations and contractual obligations. According to the PMO charter (May 25, 2004), the PMO is responsible for:

- Creating and maintaining USAID's EA and a range of technical and process standards.

- Coordinating project management activities across the Agency's major projects, driving accountability for results, and providing an effective and repeatable project implementation capability.

- Creating and implementing a PMO program of continuous self-improvement to advance the maturity of project and program management at USAID.

However, the scope of the PMO was intended to evolve as USAID improves its level of project management maturity. For this reason, the PMO was chartered to initially focus only on advising and mentoring four priority Business System Modernization projects and take on additional IT projects as the PMO expanded. Those four priority projects were (1) POD and the steady operations and maintenance of Phoenix, (2) EA, (3) PSIP, and (4) USAID's eGovernment Project Portfolio, which is intended to improve access to Internet services across agencies.

To continue the maturation of the PMO, USAID developed a Maturity Model and Implementation Plan (the Plan) to provide a framework to guide the development of the PMO, defining capability targets and measuring progress made towards the goals. According to the Plan, it is a forward-looking model for attaining project management maturity, the degree to which the PMO has acquired the tools, knowledge, and processes necessary to repeatedly complete successful projects on schedule and within budget. The Plan established three PMO target stages of maturity over the next three years:

- Stage 1: Design and Develop Project Management Standards, Tools, Templates and Processes.

- Stage 2: Implementation and Adoption of Tools, Templates and Processes across BTEC PMO project portfolio.

- Stage 3: Coordination, Integration, and Optimization of Project Management Standards, Tools, Templates, and Processes across projects.

To date, the PMO has accomplished several required actions for Stage 1. For example, it has developed some standards and documents, such as a risk management, a quality assurance plan, and a project charter template. However, the PMO remained in Stage 1 as it continued to design and develop project management standards.

According to PMO officials, because USAID did not receive funding to continue the maturation of the PMO, PMO efforts have been redirected to focus resources on (1) the USAID Administrator's priorities for Business Systems Modernization and (2) legislative and regulatory mandates that are being reinforced through the President's Management Agenda. As such, Agency officials no longer consider the PMO charter[10] or the Maturity Model and Implementation Plan to be valid documents. USAID, therefore, needs to clearly define the role of the PMO and develop a plan to implement the functions of the PMO. As such, we are making the following recommendation.

> *Recommendation No. 5: We recommend that the Director of USAID's Program Management Office prepare and implement a detailed plan (including detailed milestones, performance measures, and metrics) to establish a mature Program Management Office that provides for a repeatable project-implementation capability that analyzes, reduces, manages and mitigates project risk.*

Evaluation of Management Comments - In response to the draft audit report, USAID management agreed to develop a Project Management Plan that will address improvement/maturation of the Program Management Office (to the extent that budget and management priorities permit). The Agency also noted that an Action Memorandum has been submitted to the Administrator to create a new program office and to reorganize the Management Bureau structure to allow for the creation of this new office. Based on the above, we consider that a management decision has been reached for Recommendation No. 5.

CIO Not Provided Control To Ensure Sufficient Resources for an Effective IT Governance Structure - In February 2001, the U.S. Government Accountability Office issued an Executive Guide on "Maximizing the Success of Chief Information Officers" (the Guide) to assist Federal agencies in maximizing the success of CIO organizations. The Guide identifies principles and practices gleaned from case studies of three private and three public sector organizations recognized as leaders in successfully managing information technology investments, including the CIO function. In the Guide, the U.S. Government Accountability Office concluded that leading organizations adopt and use an enterprise-wide approach under the leadership of a CIO who has the responsibility and authority—including budgetary control—for IT across the entity.

ADS Chapter 541, "Information Management," provides the Agency's information management framework to support its mission, goals, and objectives. According to section 541.3:

> *[t]he CIO serves in a leadership role with overall responsibility and authority for approving the Agency-wide information technology budget and has overall responsibility for planning and budgeting activities for information technology-related investments that benefit USAID.*

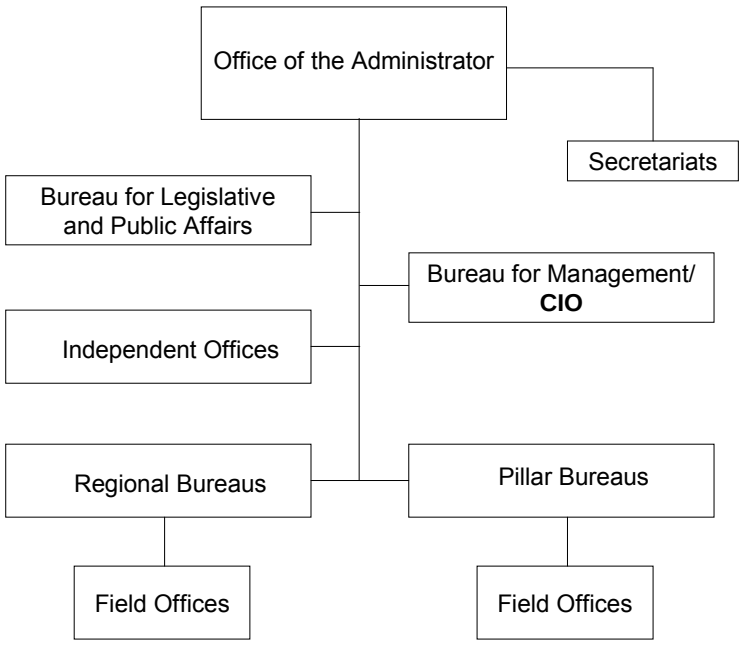
However, in practice, USAID's CIO does not have authority and control over the USAID-wide information technology budget—although such control is important for an effective IT governance structure. Instead, USAID's Bureau for Policy and Program Coordination

[10] Because ADS Chapter 101 describes the roles and responsibilities of the PMO, revising the charter is not necessary.

(PPC) is responsible for allocating resources within the Agency. Specifically, PPC's Office of Resource Allocation is responsible for allocating appropriated funds to Agency operating units. In addition, a subdivision within PPC's Office of Strategic and Performance Planning analyzes operating expense budgets, identifies resource policy issues and options, makes recommendations regarding budget levels and composition, and leads teams as needed to address specific strategy and budget issues associated with assigned operating units. Both the CIO and PPC officials have confirmed that the CIO is not involved in the Agency-wide budget process for IT.

Further, as shown in USAID's organization chart (below), the CIO is a peer to other operational officers and competes with them for resources to carry out his responsibilities.

Table 1. USAID's Organization Chart



As a result, according to USAID officials, the biggest obstacle to implementing an IT governance structure has been insufficient resources to carry out the CIO's activities needed to support the Agency. Moreover, USAID's lack of funding and human resources has hindered it in carrying out some of its critical information technology activities, such as the EA and maturing the PMO.

For this reason, the Office of Resource Allocation and the Office of Strategic and Performance Planning need to implement a process that provides the CIO the ability to examine how Agency-wide information technology resources are spent. This would provide the CIO an opportunity to ensure sufficient resources are available to carry out an effective information technology governance structure for the Agency. Therefore, we are making the following recommendation.

Recommendation 6: We recommend that the Directors of USAID's Office of Strategic and Performance Planning and Office of Resource Allocation (within

the Bureau for Policy and Program Coordination) implement a process to allow the Chief Information Officer to examine how Agency-wide information technology resources are spent in accordance with Automated Directives System section 541.3, thus allowing the Chief Information Officer the ability to ensure sufficient resources for an effective information technology governance structure.

Evaluation of Management Comments - In response to the draft audit report, USAID management agreed to modify applicable ADS sections to improve the assessment of IT systems and resources "in use" and "planned" and assure adequate resources are available for IT governance processes. Based on the above, we consider that a management decision has been reached for Recommendation No. 6.

IT Resources Not Always Used Responsibly and IT Risks Not Always Managed Appropriately - As a result of the problems in USAID's IT governance structure (discussed on pages 5-12), USAID did not always use its IT resources responsibly and manage its IT risks appropriately. Specifically, USAID experienced problems with its PSIP project and experienced some inefficiencies with its POD project. Moreover, USAID may continue to (1) have difficulty aligning its IT with the business, (2) develop its systems in a "stovepipe" manner, and (3) be unable to repeat its successes and thus maximize IT resources. The following paragraphs discuss these impacts in detail.

Problems Led to Suspension of PSIP Project – As a result of weaknesses in USAID's IT governance structure (discussed on pages 5-12, the PSIP project experienced serious problems, ultimately leading to the decision to suspend the project after spending approximately $4.3 million with no usable software to show for it. Specifically, as discussed below, USAID did not (1) ensure the software was fully developed prior to purchasing it, (2) effectively mitigate project risks, and (3) promptly respond to the results of the independent verification and validation of the project.

- **Software Not Fully Developed Prior to Purchase** – USAID's program design for its new procurement system called for the purchase of a commercial off-the-shelf (COTS) computer application.[11] A market study was conducted to determine software available to fulfill the Agency's needs. However, a decision to purchase one vendor's product was made prior to completing this selection process. Further, USAID did not test the software application before purchasing it to ensure that basic functionality for the procurement function was provided in the software package. Instead, because the software application was still in development at the time of purchase, USAID relied on claims from the software vendor that the software would include the functionality of an earlier version and operate in a web-based environment rather than a client-server environment. As a result of these decisions, USAID paid for a software application in development rather than a readily available COTS package. Moreover, although USAID spent approximately $4.3 million for integration of this software application, it did not receive a functional software application in return.

[11] COTS software or hardware products are ready-made and available for sale to the general public and are designed to be incorporated easily into existing systems. According to best practices, IT today is primarily COTS with some tailoring. Generally, the rule of thumb is that the build-or-buy break point is 80 percent COTS and 20 percent tailoring. Thus, projects should plan for 0–10 percent tailoring to allow for unanticipated growth in tailoring or new codes.

- **Ineffective Mitigation of Project Risks** - USAID did not effectively mitigate its risk for its PSIP project. Specifically, USAID identified the "inability of the web-based system to optimally perform in an overseas environment where the network support may not be adequate for the remote missions" as a high risk to the project. However, the Agency's risk-mitigation plan did not address this risk. In particular, the mitigation plan was to investigate the web-based functionality, rather than addressing concerns with system performance. Further, the mitigation plan was to focus initially on Washington, then on the missions. However, the risk was the ability of the system to perform in an overseas environment. Consequently, the risk-mitigation plan did not lower the identified risk.

- **Slow Response to Independent Verification and Validation (IV&V) Results** – The purpose of the IV&V was to, among other things, independently (1) review the PSIP processes against best practices, (2) identify PSIP program risks, and (3) provide recommendations as appropriate. The IV&V report noted that the project would have difficulty in meeting 64 gaps in mandatory requirements for the software, data, configuration and/or procedural aspects of PSIP. Such problems would pose serious risks to its performance, cost, and schedule. Though the IV&V report was released in April 2005, the report states that in January 2005, PSIP project managers were briefed on the IV&V results. Yet the project was not suspended until late April 2005—almost 5 months after PSIP project managers were made aware of these serious problems.

Shortly after USAID's new PMO Director began, the PSIP project was suspended due to the serious technical and functional issues with the software. By that time, USAID had spent approximately $4.3 million for software integration, of which $311,000 was for 1,000 usage licenses and maintenance fees. USAID continued to pay $5,200 per month in maintenance fees (which, according to USAID officials, would continue until the contract expired in September 2005), though no usable software had been delivered. (After audit fieldwork, USAID selected a different procurement package under the PSIP project.)

Some Undisciplined Practices Led to Deficiencies in POD Project Activities – According to the PMO, the POD project team adopted PMO recommended standards. However, the lack of sufficient project oversight limited the Agency's ability to ensure meaningful adoption of those standards. Consequently, USAID's internal controls were weakened in its capacity to ensure user requirements were met and project risks were effectively managed. Some of the deficiencies in the controls employed are discussed below.

- **Inadequate Contingency and Risk-Mitigation Plans for High Project Risk** – USAID identified performance problems of the system in low-bandwidth, high-latency missions as a high risk to the project. (Bandwidth is the amount of data that can be transmitted in a fixed amount of time or the capacity. Latency is the amount of time it takes a data packet to travel from source to destination. Together, latency and bandwidth define the speed and capacity of a network.)

  However, risk-mitigation and contingency plans were not fully developed to address the identified risk. (A risk plan describes the mitigation plan of specific

activities necessary to eliminate or reduce the likelihood or probability of the risk; while a contingency plan specifies a plan of specific activities that are to be executed if the triggering events occur.) Specifically, although this risk was identified at the onset of the project, the POD team did not develop its risk-mitigation strategy to improve performance in low-bandwidth, high-latency missions. In addition, although USAID identified the "possibility of reorganizing some of the overseas missions Controllers offices" as the contingency plan, it did not document a detailed plan to reorganize. This is of particular concern because the scheduled start date for deploying to the Asia Near East and Africa regions—where significant bandwidth and latency concerns have been identified—begins within the next two to six months. In response to the OIG's IT Infrastructure Audit, the Chief Financial Officer committed to finalizing a business contingency plan by November 2005. However, at the time of drafting our evaluation comments, a business contingency plan had not been provided to the OIG.

Currently, USAID has no business continuity plan in the event of disruption of service with the Washington servers. Our review of the Plan of Action and Milestones (POA&M) available during our audit fieldwork indicated that November 2005 was the planned milestone date for completing the business continuity plan. However, the necessity of having a business continuity plan in place was made evident in a recent virus attack on the Washington server. Most Phoenix users were unable to connect to the server on the day of the attack. The POD technical team measured the document-processing activity inside Phoenix and determined that the Phoenix users generated approximately 14 percent of the documents compared to before the attack. Mission users were measured at only 4 percent.

- **Data Migration Requirements Not Stable** – Although the POD team took steps to establish requirements during the planning phase of the project, its efforts did not address the needs of all key stakeholders. As a result, USAID has continually modified the data elements migrated in order to satisfy users' information needs.

  Specifically, the requirements established for the pilot and Latin America and the Caribbean (LAC) deployments included the Mission Accounting Control System (MACS) Auxiliary Ledger (MAL) extract tables, and reference data from vendor and agent/contractor tables from MACS. In November 2004, following the pilot mission deployment, a conference was held to adjust the strategy, refine the requirements, and incorporate lessons learned. The POD team learned during the conference that the data migration should be modified to include the MACS project elements data for bilateral obligations. Because the LAC deployment was accelerated from April 2005 to February 2005, project element data was not incorporated into the data migration strategy until the Europe and Eurasia (E&E) regional deployment in July 2005. However, during the LAC deployment, additional vendor data was migrated to include updated banking information.

Then, during the most recent deployment to the E&E region, in addition to the project element data, additional information from the pay file in the MACS Payment Tracking System was also incorporated into the migration.

Rather than perform a thorough requirements assessment prior to deployment, in each regional migration, additional MACS data was migrated in order to fulfill the users' needs for information. With each modification to the data elements migrated, additional programming and testing costs may be incurred to modify the migration and data validation programs and conduct the required testing.

- **System Upgrade Deployed Before It Was Ready** – The Momentum software upgrade included significant functional and technical enhancements. However, the Agency accepted and authorized moving forward with the upgrade despite the fact that (1) system and regression testing resulted in numerous open test incident reports[12], (2) some significant functionality was deferred for future releases of the software, and (3) certain reporting functionality was not system tested. The POD team's "deploy and fix" methodology became evident shortly after the upgrade. Specifically, immediately after going live with the software upgrade, the POD team prepared urgent change requests, to implement 32 needed changes that impacted several functional areas, including—but not limited to—automated disbursements, accounts payable and credit cards.

  In addition, the POD team did not conduct user acceptance testing the software upgrade, which is designed to allow users an opportunity to test the software and communicate concerns. Given the number of test incidents, the POD team should have taken steps to conduct user tests of the software as configured to ensure the software met their needs. (Helpdesk tickets showed problems with disbursements, budgets, and other significant functions of the software.)

- **Deficiencies with Data Migration, Validation and Clean-up** – The POD team's high-level phases to migrate the data were (1) configuration and set-up, (2) validation and acceptance, and (3) production and cutover. However, some problems were noted, as discussed below.

  The methodology for migrating vendor data is to migrate MACS agents[13] to Phoenix if they are used on an open obligation or commitment or if a payment has been made to the agent since fiscal year 2001. Although this methodology produced a significant number of vendor records lacking essential vendor data (such as social security numbers, tax identification numbers, and addresses), the POD team did not adjust the strategy to solve this issue. As a result, approximately 36 percent of the vendor records for the LAC region were migrated as miscellaneous vendor records. In a March 8, 2005 meeting, the Program Management Team recognized this problem noting, "Too many vendors have been categorized as miscellaneous."

[12] The Test Incident Reports were used for documenting, tracking and resolving problems identified during test execution.

[13] A MACS agent is an entity (e.g., vendor, employee) to whom USAID may make a payment. MACS agents are required to be in the MACS agent table in order for a payment to be made.

In addition, in a March 22, 2005, conference call, Agency officials in the Dominican Republic reported that they were "[r]eceiving checks from other missions because of incorrect address lines. It happened this week with Jamaica and last week with Haiti." This issue could have very serious implications in regards to the financial statements. Annually the Agency is required to estimate and report the amount of erroneous payments for activities where the risk is significant.

According to the Data Migration Validation Plan, the Validation team is responsible for validating that the reference tables are populated correctly and the transaction data are accurate. In other words, data validation is done to ensure data integrity is maintained. For the mission data validation, the crosswalks between MACS/MAL and Phoenix data elements are used to translate historical and current-year MAL transactions accurately into Phoenix. The Data Migration Validation team validates that the crosswalks and corresponding data are mapped accordingly in the Phoenix system. However, the LAC production validation results noted that, because the MAL records were not cross-walked to the appropriate Phoenix table, (1) the error rate for advances and advance liquidations of three missions exceeded the 2 percent threshold and (2) the error rate for disbursements for non-"advice of charge" exceeded the acceptable error rate of 2 percent for two missions.

Finally, regarding data clean-up, rather than providing a remedy to correct some data, the Data Migration team recommended that LAC exclude certain data from the migration—a recommendation that LAC accepted. By taking this approach of not migrating problem data, the POD team is at risk of excluding essential data that may be needed in the future.

- **Difficulty Meeting Critical Reporting Needs** – Although reporting was identified as a high risk to the project, the POD team did not take appropriate measures to ensure that reporting needs would be met. Specifically, the team did not (1) effectively develop reporting requirements, (2) perform adequate user acceptance tests of the reports before implementing them, and (3) complete their operational readiness checks with respect to reports before going live. As a consequence, the POD team experienced extreme difficulty meeting the critical reporting needs of mission users.

Unfortunately, the Agency's current governance structure, inadequate policies and procedures and lack of adequate resources in the PMO, staged the current scenario for the POD project to monitor itself. The lack of objective, independent project oversight for the POD project limits USAID's ability to ensure that best practices are implemented as described in copious documentation. Without enterprise-level policies and standards, USAID will continue to subject itself to an endless cycle of ad-hoc implementation practices driven by aggressive deployment schedules.

Difficulty Aligning IT with Business – An IRM Strategic Plan should support the Strategic Plan of the Agency and guide all IT investments to ensure they enable the business of the Agency. By not having an updated IRM Strategic Plan—a fundamental component needed to successfully modernize its business systems—USAID will have difficulty aligning its IT with identified needs and priorities for addressing the challenges that the Agency will face over the next five years. Specifically, USAID will have difficulty

integrating its IRM decisions with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

Systems Developed in a "Stovepipe" Manner – An EA should provide a strategy that will enable the Agency to support its current state and also act as the roadmap for transition to its target environment. The primary purpose of the data reference model component of an EA is to promote the common identification, use, and appropriate sharing of data/information across the Federal government. At USAID, the PMO should serve as the body that ensures data from all projects are integrated/shared across the Agency.

However, because the EA not being fully developed and the PMO was not fully functional, USAID continues to build its systems in a "stovepipe" manner. Specifically, there is no assurance that the data collected and the information reported by these systems will be able to be shared across different systems. Further, there is no assurance that duplicate data will not be collected and stored—resulting in inefficiencies and possible disparities.

One such example is the PSIP and POD projects. The accounting system (deployed by the POD project) will contain some contract and obligation data (e.g., vendor name and award amount), which will also be contained or referenced by the procurement system (deployed by the PSIP project). Although USAID reviewed project interdependencies and established a committee to (among other functions) guide, at the executive-level, the planning and implementation of USAID's core accounting and procurement systems in USAID/Washington and overseas missions, the projects are being managed in a "stovepipe" manner. For example, although PSIP required a future version of the software, the POD project moved forward in deploying an earlier version, rather than ensuring that the needs of both systems would be met.

Finally, the accounting and procurement systems will need to be integrated at some time in the future—which will lead to additional costs. Moreover, both projects are being developed and implemented without the benefit of an EA. The goal of an EA is to define, maintain, and implement an Agency-wide roadmap that achieves an Agency's mission through optimal performance of its core business processes within an efficient IT environment. The lack of this roadmap may result in the interdependencies between PSIP and POD not being identified—resulting in inefficient business operations and underlying IT support operations.

Another example of a problem caused by this "stovepipe" manner of developing systems can be found in the relationship between the Executive Information System (EIS) and EA Projects. The purpose of the EIS is to collect data and use it to generate information needed to operate the Agency and report results to customers inside and outside of the Agency. Similarly, the primary purpose of the EA project, in its data reference model, is to promote the common identification, use, and sharing of data/information across the Federal government and within the Agency. Therefore, the two projects are interrelated and should be coordinated or integrated. Yet they are not because the interrelations were not managed due to their "stovepipe" structure. The EA has been managed by the PMO, and the EIS had been managed outside the PMO by a member of the CIO's staff—with little PMO involvement. (After OIG inquiries, the EIS was recently placed under the auspices of the PMO.)

In summary, USAID's IT initiatives address the requirements of one "stovepipe" application, but does not consider requirements that overlap multiple projects. Therefore, USAID is at risk that the enterprise-wide requirements may not be satisfied in the individual applications.

Inability to Repeat Successes and Thus Maximize IT Resources – Because USAID did not fully establish its policies and procedures at the enterprise level, its projects have relied on the methodologies of its contractors for many activities. As a result, the successes of the projects are not necessarily a repeatable process for the Agency as a whole and, therefore, other IT initiatives may not be able to benefit from those successes—unless other projects engage the same contractors. Moreover, other IT initiatives may need to "reinvent the wheel"—costing additional time and money to implement the projects. For example, even though the POD project experienced some problems, to date USAID has implemented the system at 22 missions. However, those successes may not necessarily be repeatable for the Agency.

Conclusions - An effective IT governance structure is essential for USAID to meet the goals of its Business Transformation Plan to reform the Agency's management systems and improve organizational performance. In order to meet its desired transformations, USAID must (1) align its IT with the business, enable the business and maximize resources; (2) use its IT resources responsibly; and (3) appropriately manage IT risks. Moreover, USAID's reputation may not survive another major unsuccessful attempt to deploy its management systems. As such, we are making recommendations to help USAID improve its information technology (IT) governance and thus reduce the risks involved in Agency IT initiatives. Further, our recommendations will help USAID to correct its longstanding material weakness in its Information Resource Management processes.

EVALUATION OF MANAGEMENT COMMENTS

USAID's Acting Chief Information Officer (CIO) and the Acting Director of Resource Allocation prepared a consolidated written response to our draft report. The consolidated response is included in its entirety in Appendix II of this report.

In their response, USAID agreed with and plans to take action on all six recommendations. A summary of USAID's comment and our evaluation follows each recommendation in the body of the report. Based on USAID's response, a management decision has been reached on Recommendation Nos. 1, 2, 3, 4, 5 and 6.

In addition to the responses provided for our recommendations, the Agency prepared written technical comments on the effects of project risks reported. The following section provides our evaluation of the Agency's technical comments. Where appropriate, we made changes to the report.

The Agency technical comments begin by stating, "We are pointing out what may be factual inaccuracies." However, as shown in our analysis below, we believe that their comments did not point out any factual inaccuracies.

- Page 12, Fourth Paragraph: In its comments, USAID management stated, "Characterization of the PSIP Project as "Unsuccessful" is entirely incorrect and premature." The term "Unsuccessful" only appears in the subheading to this report segment as "Unsuccessful PSIP Project." In response to management concerns this subheading was changed to "Problems Led to Suspension of PSIP Project" to more closely match the report text. However, in its comments management acknowledged that, in Fall 2005, it selected a new acquisition and assistance systems "to ensure that the delivered COTS product met the needs of the Administrator's mandate and the user community for acquisition and assistance actions." This action resulted from management having suspended the PSIP project after abandoning further development of the "COTS" product initially selected.

- Page 13, First Paragraph: In its comments, USAID management stated, "Reference to software not fully developed prior to purchase is an inaccurate characterization of the COTS product." However, based on the following facts, we concluded that the report's characterization of the software as not fully developed prior to purchase is correct.

  In reference to COTS, the USAID PSIP Implementation Plan, states that the project, "emphasizes the use of Commercial-off-the-shelf (COTS) products − minimizing the need for extensive software development." However, as previously noted, in Fall 2005 USAID purchased alternative software due to shortcomings in the software initially selected. In its own comments regarding the software initially selected management states "there were significant risks associated with the product's

reliability and stability in the new technical platform. USAID felt that these risks were too great to continue and conducted an analysis of alternate solutions to determine if other systems better met USAID's needs out of the box."

Our conclusion, also stated by management, was that "out of the box" the software initially selected required more than minimal software development.

- Page 13, Second Paragraph: In its comments, USAID management stated, "The PSIP Team disagrees with the assessment that USAID did not effectively mitigate its risk for the PSIP project." However, management's comments present only a hypothetical description of actions that would have been taken had the project not been suspended. Specifically, management stated that the intent was to conduct tests in Washington and later develop a mitigation strategy for overseas. This comment alone shows that USAID did not mitigate its high risk for PSIP, which was "the inability of the web-based application to optimally perform in an overseas environment where the network support may not be adequate for remote missions."

- Page 13, Third Paragraph: According to USAID's management comments, the PSIP Team disagrees with the assessment that their response to the Independent Verification and Validation results was slow. However, as noted in the audit report, in January 2005, PSIP managers were briefed on the initial Independent Verification and Validation results—which identified the same requirements gaps in the April 2005 final report. Specifically, the Independent Verification and Validation determined that the software would not meet 64 key requirements. Instead, USAID continued with the project until shortly after USAID's new Project Manager Director began.

- Page 13, Fourth Paragraph: In its comments, USAID management stated, "For clarification, the continuance of the $5,200 was for software maintenance fees." Further, management stated that the continuance of those payments were necessary to ensure the future use of the software, if needed. USAID management's clarification is noted. Thus, we changed the report to reflect "maintenance" fees rather than "licensing" fees. However, as stated in the report, implementation of the prior software was abandoned. This resulted in the payment of additional maintenance fees of $26,000 that were of no use.

- Page 14, Fourth Paragraph – Management stated that our characterization that their contingency and risk-mitigation plans for the POD project as inadequate is not entirely accurate because both risk mitigation and contingency plans have been developed and adopted by the missions. Management further responded that the risk mitigation plan is to purchase additional bandwidth to mitigate potential network connectivity performance issues and the World Wide Vouchers Examiner (WWVE) strategy serves as the business contingency plan. Because the information provided in management's response was not provided during our fieldwork we were unable to review and test the adequacy of the contingency and risk-mitigation plans. In addition, because management's response did not include the date the risk mitigation and contingency plans were developed it is unclear if these strategies were in effect at the time that our audit fieldwork was being conducted. The Agency also stated that in their analysis of Help Desk Remedy Tickets, Phoenix is functioning at an acceptable level of performance. Although we did not evaluate

system performance in this audit, in a February 2005 audit report,[14] we recommended USAID (1) develop and implement formal performance goals for transaction response times in Phoenix in all worldwide locations and (2) implement a process to actively monitor transaction response times in Phoenix in all worldwide locations. To date, USAID has not taken final corrective action on either recommendation. Nonetheless, this does not preclude the need for a contingency plan.

In addition, management pointed out that in their response to our February 2005 audit report,[15] the Chief Financial Officer committed to finalizing a business contingency plan. Although not stated in management's response to this report, the CFO's plan was targeted to be completed by November 2005. At the time of drafting our report, we had not been provided a copy of management's business contingency plan. We have provided additional information in this report to explain that the contingency plan had not been provided.

Management further stated that a finalized contingency plan was not critical until after the Asia and Near East (ANE) deployment. Management correctly pointed out that based on our findings during the IT Infrastructure Audit; the IG found that the connectivity between pilot and LAC missions was reliable. However, we disagree that a finalized contingency plan was not critical until after the ANE deployment. As stated in our report, a contingency plan specifies a plan of specific activities that are to be executed if the triggering events occur. In accordance with Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources and the Paperwork Reduction Act, contingency planning for major applications are required as a part of the Application Security Plan and should be incorporated into the strategic IRM plan prior to the security plan's implementation.

- Page 14, Fifth Paragraph – Management disagreed with the statement in our report that USAID had no business continuity plan in the event of disruption of service with the Washington servers. Management stated that "POD had an actionable continuity plan in place, based on the Department of State's Beltsville Information Management Center (BIMC), in case USAID servers experienced a disruption in service." Our review of the Plan of Action and Milestones (POA&M) available during our audit fieldwork indicated that November 2005 was the planned milestone date for completing the business continuity plan. We have revised our report to include the November 2005 milestone for completing business continuity plan.

- Page 14, Sixth Paragraph and Page 15, Second Paragraph – Management objected to our conclusion that the data migration requirements were not stable and stated that our statements were not entirely accurate. We understood and took into consideration the need for adjustments to the data migration strategy based on lessons learned from the pilot deployment. However, our audit found that USAID's subsequent adjustments to the migrated data were due in part to the difficulty in meeting reporting requirements—which impacted the migration effort. For example,

[14] Audit of USAID's Information Technology Infrastructure (Report No. A-000-05-006-P, February 22, 2005)

[15] Ibid, footnote 14

according to the February 2005 edition of the "Phoenix Flight," the Reports Team refined the data migration strategy after deploying Phoenix to the LAC region. The purpose of the refinement was to add "MACS program element" under bilateral agreements, which would provide more detailed reports to users. Moreover, this refinement was made to solve some of the reporting problems that users were experiencing.

- Page 15, Third Paragraph – Management pointed out that test incident reports (TIRs) are not equivalent or necessarily translate to change requests (CRs). We agree that it is possible that TIRs do not necessarily translate to CRs. However, to clarify our point, we revised our report to state that:

  > …the Agency accepted and authorized moving forward with the upgrade despite the fact that 1) system and regression testing resulted in numerous open test incident reports[16], (2) some significant functionality was deferred for future releases of the software, and (3) certain reporting functionality was not system tested.

- Page 15, Fourth Paragraph - Management accurately pointed out that user acceptance testing is not required under industry best practices for TIRs and/or to address software changes/upgrades, when system and/or regression testing is performed. However, in our opinion, user acceptance tests of the system functionality and reports should have been conducted given the results of the system and regression test results.

- Pages 15-16, Sixth Paragraph – Management objected to the presentation of information related to the effect of data migration deficiencies identified during the audit. In response to management's comments we have revised the report to include our findings regarding erroneous payments in a separate paragraph for clarity to the reader.

- Page 16, Second Paragraph – Management did not agree with our statement that "the POD team is at risk of excluding essential data that may be needed in the future" because "the Data Migration team recommended that LAC exclude certain data from the migration." The basis for our concern with the data clean-up process was to address one of the difficulties the Agency has experienced in the past in reporting accurate and timely data for congressional data calls. In our opinion, excluding data from the data migration as a strategy to address the data clean-up process will not improve the Agency's ability to provide accurate and timely information.

- Page 16, Fifth Paragraph – Management stated that the comment in our report regarding the lack of adequate resources was not entirely accurate. Our audit found a lack of objective or independent project oversight. As stated in our report, we found a lack of adequate resources in the PMO to provide independent project oversight. In response to managements concerns we will include the word "independent" in our comment for clarity to the reader.

[16] The Test Incident Reports were used for documenting, tracking and resolving problems identified during test execution.

- Page 17, Fourth Paragraph – In our report, we used POD and PSIP projects as an example of USAID developing its IT systems in a stovepipe manner. In response, management commented that "senior officials made it clear that the priority was to deploy Phoenix overseas" and that stopping the POD project to wait for PSIP would cause the POD schedule to slip and budget to increase. However, we did not state that the POD project should have stopped to wait for PSIP. Instead, our comment was to show that decisions for the POD project—in this example the software version—were made without considering the needs of both projects.

- Page 18, Third Paragraph – Management commented that our statements related to the POD project success not being repeatable for other USAID projects were not entirely accurate. Management supported their comments by pointing out the Phoenix program management processes and procedures, such as the Risk Management Plan, Quality Assurance Plan, Communications Strategy and Plan, project and team charters, have been leveraged by other USAID business systems initiatives such as JAMS and PSIP. In the report, we stated that the Agency adopted risk management and quality control plans into its IT initiatives at the Agency level. However, in our opinion the lack of enterprise level policies and procedures hampers the agencies ability to repeat the same processes in other areas such as developing requirements, data definitions, and system's testing.

SCOPE AND METHODOLOGY

Scope

The Office of Inspector General, Information Technology and Special Audits Division, performed this audit in accordance with generally accepted government auditing standards. The purpose of the audit was to determine whether USAID used Federal requirements and best practices to implement an integrated process to manage and control its Phoenix Overseas Deployment (POD) and Procurement System Improvement Program (PSIP) projects. Audit fieldwork was conducted at USAID headquarters in Washington, D.C., from March 3, 2005, through August 22, 2005.

Although we focused primarily on USAID's IT governance over its POD and PSIP IT initiatives, we also considered the enterprise architecture and the Executive Information System IT initiatives as they related to POD and PSIP. As such, for the enterprise architecture and Executive Information System, we performed only limited audit work.

To conduct the audit, we considered some IT processes within USAID's:

- Identification of the way IT can best contribute to the achievement of the business objectives.
- Identification, development or acquisition of systems as well as the implementation and integration of those systems into the business processes.
- Actual delivery of required services.
- Monitoring of IT processes for their quality and compliance with control requirements.

However, we did not include IT security within the scope of our work.

Methodology

As the framework for designing this audit, we used the July 2000 edition of the Control Objectives for Information and related Technology (released by the COBIT Steering Committee and the IT Governance Institute). Based on initial interviews and reviews of documentation, we used our judgment to select which control areas were most critical to USAID's IT governance process. Further, we tailored the suggested audit procedures to USAID's environment.

We interviewed direct hires and/or contractors from USAID's Office of the Chief Information Officer, including the Office of Information Resources Management and the Program Management Office. In addition, we interviewed direct hires and/or contractors from USAID's Office of Financial Management and the Office of Acquisition and Assistance, who were responsible for the POD and PSIP projects, respectively.

We reviewed relevant laws, regulations, best practices, and USAID policies, procedures,

and guidance. We also reviewed Agency plans and documentation from the PMO as well as from the PSIP and POD projects, including, but not limited to charters, plans, and contracts. Finally, we reviewed results of other audits and reviews related to our audit objective.

Using the above information, we identified areas that we perceived as high risk based on the significance and sensitivity of that process and the likelihood that the particular process may not achieve its intended control objective. For those high-risk areas, we performed tests to assess the adequacy of the IT controls. However, this audit was not sufficient to make definitive determinations of the effectiveness of IT controls that were not considered to be high risk.

A specific materiality threshold was not set for the audit. Instead, we used our judgment in determining sampling sizes to assess the Agency's IT governance.

MANAGEMENT COMMENTS

January 13, 2006

MEMORANDUM

TO: IG/A/ITSA, Melinda G. Dempsey

FROM: M/CIO (Acting), John Streufert /s/
PPC/RA/PBI, Patricia Sommers /s/

SUBJECT: Management Response to Office of Inspector General's Report: *Audit of USAID'S Information Technology Governance Over its Phoenix Overseas Deployment and Procurement System Improvement Program Projects (Draft Report No. A-000-06-00X-P, October 27, 2005)*

Thank you for the opportunity to respond to the subject draft report. We appreciate your review and are providing our comments, other relevant information, and management decisions on the recommendations in the report.

We feel that it is important to provide you with the current context impacting the future of Information Technology Governance at USAID. The Office of Management and Budget (OMB) has consistently expressed support for enhanced strategic and operational collaboration between the Department of State (State) and USAID. Both State and USAID have been directed by OMB to use the Joint Enterprise Architecture as the vehicle for mapping the business functions of both organizations and identifying potential areas of duplication and realignment. OMB has instructed that the Joint Management Council (JMC) be responsible for prioritizing the functions to be examined and ensuring that transparent and actionable

implementation processes are in place to systematically drive business process change and produce results. OMB has further called for the establishment of a Joint Program Management Office (JPMO) that would report to the JMC to govern the execution of the Enterprise Architecture and its implementing projects. To encourage adoption of their recommendations, OMB has not supported funding the USAID Enterprise Architecture or the USAID PMO in either FY06 or FY07. Additionally, the AA/M has recently sent an Action Memorandum to the Administrator recommending approval to create a new program office for more effective and efficient management of Management (M) Bureau resources and to reorganize the M Bureau structure to allow for the creation of this new office. The extent of the impact on the existing Program Management Office is yet to be determined. Pending decision on the M Bureau reorganization and the formalization of the joint State-USAID management structures and funding approach, USAID is able to continue a modest investment in improving IT Governance at USAID utilizing PMO Capital Investment Funds allocated in FY05. Future process improvement activities will be supported to the level that available funding and resources can be provided and management priorities permit.

Management Decisions

Recommendation No. 1: We recommend that the Chief of the USAID Program Management Office's Business Enterprise Architecture Division develop and implement a plan to address the enterprise architecture needs of the Agency.

Management Decision: The development and the implementation of the Joint Enterprise Architecture are currently being managed by the Department of State. The Joint Enterprise Architecture Completion and Use Plan Progress Report submitted to OMB by Department of State in May 2005 provides a summary of the current status and planned actions for the JEA. In support of the Executive Information System (EIS) project, M/PMOBEA shall develop a data reference model (DRM) focusing on the data that supports the program and activities management (April 2006). Unaddressed elements of the DRM, along with other reference model information will be developed as budget and management priorities permit . The Business Enterprise Architecture Division, in concert with the Enabling Technologies and Integration Division, will develop a project plan that will address USAID's EA objectives (April 2006).

Recommendation No. 2: We recommend that the Chief of the USAID Program Management Office's Enabling Technologies and Integration Division develop USAID's policies and procedures for each phase and activity of the Agency's project life cycle, including performance metrics and measures.

Management Decision: The Enabling Technologies and Integration Division of the PMO was reorganized under the Office of Information Resources Management effective November 27, 2005. The M/IRM/ETI Division Chief will coordinate the development of USAID's IT Project Management Control Manual (PMCM) that will describe the policies and procedures for each phase and activity of the Agency's IT project life cycle and address performance metrics and measures. This manual will be a mandatory reference to the ADS. (September 2006)

Recommendation No. 3: We recommend that the Chief of USAID Program Management Office's Enabling Technologies and Integration Division prepare Agency policies and procedures for preparing Office of Management and Budget Exhibit 300s to require that documentation be maintained for cost estimates and that the cost estimates be validated.

Management Decision: The M/IRM/ETI Division Chief will develop guidance for preparing IT system life cycle cost estimates and their validation. This guidance will be a mandatory reference to the ADS. The Earned Value Management policies and procedures developed in response to Recommendation No. 4 will also include the requirement for validation of major investment performance baselines. The USAID Earned Value Management Guide to be referenced in the policy will require formal change control of performance baselines. (September 2006)

Recommendation No. 4: We recommend that the Chief of the USAID Program Management Office's Enabling Technologies and Integration Division codify USAID's policies and procedures for project risk management, quality control, and earned value management in accordance with USAID's Automated Directives System Chapter 501.

Management Decision: The M/IRM/ETI Division Chief will develop and codify USAID's policies and procedures for IT project risk management, quality control, and earned value management in the ADS.

(September 2006)

Recommendation No. 5: We recommend that the Director of USAID's Program Management Office prepare and implement a detailed plan (including detailed milestones, performance measures, and metrics) to establish a mature Program Management Office that provides for a repeatable project-implementation capability that analyzes, reduces, manages and mitigates project risk.

Management Decision: An Action Memorandum has been sent to the Administrator recommending approval to create a new program office for more effective and efficient management of M Bureau resources and to reorganize the M Bureau structure to allow for the creation of this new office. The extent of the impact on the existing Program Management Office is yet to be determined.

The Program Management Office (PMO) will develop a Project Management Plan (PMP) that will address improvement/maturation of the PMO (to the extent that budget and management priorities permit). The PMO Director has awarded a task order under the PRIME 3.1 BPA to ICOR Partners, LLC for IT Governance and PMO support. The scope of the task order includes the development of an IT Governance Management Model and progress toward its implementation. The Task Order Management Plan must be refined to reflect the impacts of the proposed M Bureau reorganization and to address current priorities which include responsiveness to these audit findings. The PMO Director or alternate CIO-designated manager will provide the revised IT Governance and PMO Support Task Order Management Plan, as modified, including detailed milestones, performance measures and metrics. (February 2006).

Recommendation 6: We recommend that the Directors of USAID's Office of Strategic and Performance Planning and Office of Resource Allocation (within the Bureau for Policy and Program Coordination) implement a process to allow the Chief Information Officer to examine how Agency-wide information technology resources are spent in accordance with Automated Directives System section 541.3, thus allowing the Chief Information Officer the ability to ensure sufficient resources for an effective information technology governance structure.

Management Decision: The Paperwork Reduction Act and Division E of

the Clinger-Cohen Act of 1996 (also known as the Information Technology Management Reform Act) require that information resources management operations and decisions be integrated with organizational planning, budget, financial management, human resources management, and program decisions. The Chief Information Officer (CIO) is required to provide advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of Division E of the Clinger-Cohen Act of 1996, consistent with chapter 35 of title 44, United States Code, and the priorities established by the head of the executive agency.

As amplified by OMB Circular 130, Section 9a (3), the CIO's role is to "be an active participant during all agency annual budget processes." The CIO is fulfilling that role at USAID. The Agency's budget is developed and approved with many internal and external stakeholders, including Congress and the White House, based on many competing priorities. The IT budget is only one of the factors that have to be considered in the negotiation of the Agency's budget.

The Chief Information Officer and Directors of USAID's Office of Strategic and Performance Planning and Office of Resource Allocation (within the Bureau for Policy and Program Coordination) will modify the Automated Directives System (ADS) Chapter 541, "Information Management", and others as required to improve the assessment of IT systems and resources "in use" and "planned" and assure adequate resources are available for IT governance processes (to include analysis, documentation, execution, control, and oversight). This will be accomplished in two stages by documenting the systems in use and planned as part of the annual budget call for estimates by PPC with a list of systems that the CIO will provide missions. With that data the CIO will analyze whether there are sufficient resources to ensure effective governance in consultation with PPC. In addition, the Agency will continue its efforts to ensure sufficient resources for IT requirements. However, ultimately the total level of resources available to USAID for all operating costs is determined by Congress and IT must be balanced against other requirements. (September 2006)

Technical Comments on Report

We are pointing out what may be factual inaccuracies. These are being provided for your consideration in an effort to strengthen your report on this very complicated and sensitive issue, especially considering the widespread interest this audit may generate.

- Page 12, Fourth Paragraph: Characterization of the PSIP Project as "Unsuccessful" is entirely incorrect and premature. The decision to suspend its implementation schedule was to allow the project team to reassess its implementation strategy to ensure that the delivered COTS product met the needs of the Administrator's mandate and the user community for acquisition and assistance actions. Unsuccessful would have been to allow the project to continue on its current course, expending scarce resources to meet a delivery schedule that may not result in meeting the Agency's functional requirements, and increase project life cycle costs. As a result of the OMB mandate to partner with the Department of State for the assistance component under the Joint Assistance Management System (JAMS), USAID made the decision to separate the JAMS and PSIP projects to more effectively satisfy the mandatory requirements for each component while still meeting the OMB mandate for JAMS. Selections of the new assistance and acquisition systems were made in the Fall 2005. A substantial amount of the integration services that were performed for PSIP are being re-used with the new JAMS and PSIP implementations, including the business process flows, data migration, reporting requirements, and some components of the system configuration. Additionally, work that was performed to integrate NMS A&A with Phoenix will also be reused to design and develop the interfaces between the new assistance and acquisition systems and Phoenix.

- Page 13, First Paragraph: Reference to software not fully developed prior to purchase is an inaccurate characterization of the COTS product. USAID conducted a market survey which identified several COTS products that met the basic functionality for acquisition and assistance. Additionally, the Department of State (State) provided USAID a demonstration of their COTS procurement system to highlight how they process their procurement transactions. The Department of State was planning to migrate from Procurement Desktop to Momentum Acquisitions to coincide with their financial migration to Momentum

Financials. At the time, USAID was also in the process of deploying Momentum Financials.

Out of the box, the COTS solution provided the basic procurement functionality and was very immature in its client base. The undeveloped part was the data and field names to support the assistance business processes. We were aware that certain requirement gaps would be addressed in subsequent releases of the software, through product customization, or through substantial business process reengineering. Given that USAID and State were the first set of agencies to deploy the web-version of the COTS product, there were significant risks associated with the product's reliability and stability in the new technical platform. USAID felt that these risks were too great to continue and conducted an analysis of alternate solutions to determine if other systems better met USAID's needs out of the box.

- Page 13, Second Paragraph: The PSIP Team disagrees with the assessment that USAID did not effectively mitigate its risk for the PSIP project. The initial phase of PSIP implementation was for domestic deployment. While configuring the COTS solution, the PSIP mitigation strategy and plan was to leverage on-going performance testing conducted by IRM and FM, and deployment of the COTS solution to missions and posts with known bandwidth and connective issues. In the meantime, PSIP had planned to conduct controlled tests to determine specific PSIP functionality with the domestic configured system, such as document generation and printing. The results of these performance tests were to help develop the mitigation strategy for overseas deployment. However, PSIP was preempted from executing the strategy when the decision was made to suspend the implementation.

- Page 13, Third Paragraph: The PSIP Team disagrees with the assessment that their response to the Independent Verification and Validation results was slow. PSIP commissioned an Independent Assessment to identify or validate key issues, risks, and recommendations. The assessment noted there were 64 mandatory requirements unresolved to be delivered. The recommendation was to develop a plan to facilitate a timely resolution of the gaps. The functional team had begun to reevaluate and reprioritize the requirement gaps based on functional, technical, schedule, and cost impact. The process of mitigating those requirements was through business process reengineering, deferring the requirements in future

version releases, or customization. The suspension decision was based on information that became known during April 2005. The notification by the vendor that the version which Phoenix was going to deploy was not a production candidate for PSIP. In addition, further technical issues were identified during systems testing and the level of effort estimates to address the requirement gaps through complex extensibility exceeded expectations. The elevated set of risks prompted the decision to suspend and notification was made on May 6, 2005.

- Page 13, Fourth Paragraph: For clarification, the continuance of the $5,200 was for software maintenance fees. At the time of suspension in May 2005, it was unclear if the project would resume with the same COTS solution and such a decision would not be known until September 2005. If USAID discontinued payment of the maintenance fee and it was determined that the project resumed with the same COTS solution, USAID would not have benefited from any version upgrade or patches to be in sync with the financial version.

- Page 14, Fourth Paragraph: Reference to an under-developed and/or inadequate risk mitigation plan for POD is not entirely accurate. The POD team developed and communicated the purchase of additional bandwidth as a mitigation strategy to missions via email, Phoenix flights, and teleconference calls. Missions in turn, adopted recommended strategy by purchasing additional bandwidth to mitigate potential network connectivity performance issues. Missions' bandwidth purchases are documented in the NECS website (http://206.118.162.10/search.asp). Based on a Help Desk Remedy Ticket analysis, Phoenix is functioning at an acceptable level of performance in all pilot, LAC, and E&E controller missions.

- Page 14, Fourth Paragraph: Reference to an under-developed and/or inadequate contingency plan is not entirely accurate. The World Wide Vouchers Examiner (WWVE) strategy was developed as an initial contingency plan for POD, and was communicated to overseas controller missions. Should a mission experience network connectivity issues, the WWVE would be granted temporary authority to approve payments on behalf of another mission, which differs from the regular Phoenix operating environment where accountants, voucher examiners, etc. are limited by security roles.

Further, it should be noted that in response to the IG's IT Infrastructure Audit (Report No. A-000-05-00X-P), the Office of the CFO committed to finalizing a business contingency plan. Performance testing between the overseas missions and USAID/W indicated that connectivity between pilot, LAC, and E&E missions and USAID/W was reliable. A finalized contingency plan would not be critical until after the Asia and Near East (ANE) deployment.

- Page 14, Fifth Paragraph: We do not agree with the assertion that "USAID has no business continuity plan in the event of disruption of service with the Washington servers." POD had an actionable continuity plan in place, based on the Department of State's Beltsville Information Management Center (BIMC), in case USAID servers experienced a disruption in service. Because this was a virus attack, the Agency did not operate Phoenix from BIMC since the virus could have been spread from USAID to the State Department via Phoenix. In addition, Phoenix was unavailable for only two days.

- Page 14, Sixth Paragraph and Page 15, Second Paragraph: Reference to the POD team not performing a requirements assessment prior to deployment and modifying migration data elements to meet stakeholders' needs is not entirely accurate. The data migration team thoroughly assessed users' information requirements and established stakeholders' requirements prior to deployment. However, based on lessons learned assessments post-deployment, data migration strategy was refined in future deployments to more effectively address users' information needs. Controllers signed off in agreement to the enhanced strategy in all instances.

- Page 15, Third Paragraph: Please note that test incident reports (TIRs) are not equivalent or necessarily translate to change requests (CRs). All TIRs classified as "high" have to be addressed and closed immediately, and all "medium" TIRs must have a clear plan of action and a proposed completion date with government approval.

- Page 15, Fourth Paragraph: Please note that, based on industry best practices, user acceptance testing (UAT) is not required for TIRs and/or to address software changes/upgrades, when system and/or regression testing is performed.

- Pages 15-16, Sixth Paragraph: The documentation provided during the audit shows that approximately 36% of total LAC vendor transactions were migrated as miscellaneous, however this is not linked to the IG's supposition that this would lead to erroneous payments. Based on the Data Migration Strategy and Plan, some vendors were migrated as miscellaneous if the vendor had no disbursement activity in the previous two calendar years and was not recorded on an open obligation. Additionally, essential vendor information/record was still captured and migrated to Phoenix.

  As a result, we do not agree with the assertion that the migration of vendors as miscellaneous leads to serious implications to the Agency's financial statements or to erroneous payments, neither of which have been reported.

- Page 16, Second Paragraph: We do not agree with the assertion that "the POD team is at risk of excluding essential data that may be needed in the future" because "the Data Migration team recommended that LAC exclude certain data from the migration." The bureau and the missions all agreed, and signed-off, on the data migration approach for the LAC missions based on their understanding of their own business operations. There is nothing to indicate essential data that may be needed in the future was excluded based on the data migration approach. Historical transactions are in MACS for research purposes and LAC missions are operating successfully on Phoenix with the data that was migrated.

- Page 16, Fifth Paragraph: Reference to inadequate resources to monitor the progress of the POD project is not entirely accurate. SRA and IBM have been supporting the management of the Phoenix project by providing project oversight based on industry best practices.

- Page 17, Fourth Paragraph: The Phoenix team began planning the overseas deployment in June 2003 and senior officials made it clear that the priority was to deploy Phoenix overseas. PSIP would trail Phoenix and adopt, if possible, the software used by Phoenix. To stop the Phoenix overseas deployment and wait for PSIP to determine what software they would use would cause the Phoenix budget to increase and the schedule to slip.

- Page 18, Third Paragraph: Reference to POD successes not being repeatable for other USAID projects due to the heavy reliance on contractors is not entirely accurate. Phoenix program management processes and procedures, such as the Risk Management Plan, Quality Assurance Plan, Communications Strategy and Plan, project and team charters, have been leveraged by other USAID business systems initiatives such as JAMS and PSIP.

We respectfully request that the comments above are addressed and/or incorporated in the final subject audit report.

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