USAID
FROM THE AMERICAN PEOPLE

OFFICE OF INSPECTOR GENERAL

AUDIT OF USAID's IMPLEMENTATION OF INTERNET PROTOCOL VERSION 6

AUDIT REPORT NO. A-000-08-006-P
September 4, 2008

WASHINGTON, DC

Office of Inspector General

September 4, 2008

MEMORANDUM

TO: Acting Chief Information Officer, Phil Heneghan

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

SUBJECT: Audit of USAID's Implementation of Internet Protocol Version 6 (Audit Report No. A-000-08-006-P)

This memorandum transmits the Office of Inspector General's final report on the subject audit. The report contains no recommendations. In finalizing the report, we considered your written comments on our draft report and included those comments in their entirety in appendix II of this report.

I appreciate the cooperation and courtesies extended to my staff during this audit by members of your office.

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

CONTENTS

SUMMARY OF RESULTS

Internet Protocol (IP) addresses are a fundamental part of the Internet. Every device connected to the Internet needs an IP address that is represented by a unique number. Currently, two types of IP addresses are in active use worldwide: IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 is the most commonly used version in the United States, with the capacity to support about 4.3 billion unique addresses. IPv6 was developed to address concerns over expected emerging demands for limited IPv4 addresses. Although differing views exist within the Internet industry as to the pace of demand for the remaining IPv4 addresses, demand for IP addresses is expected to increase as more and more of the world's population requests Internet access and uses electronic devices that require an IP address. IPv6 is intended to meet this future demand with a capacity to support about 3.4×10^{38} unique addresses. Consequently, use of both IPv4 and IPv6 is expected to overlap for some time. The hardware and software infrastructure needed to support both IPv4 and IPv6 presents a challenge to the Federal Government (page 3).

To guide Federal Government agencies in their transition to IPv6, in August 2005 the Office of Management and Budget (OMB) issued memorandum M-05-22, "*Transition Planning for Internet Protocol Version 6 (IPv6)*," which outlined a transition strategy for agencies to follow and established the goal for all Federal agency backbone[1] networks to support IPv6 by June 30, 2008 (page 3).

The Office of Inspector General, Information Technology and Special Audits Division, in Washington, DC, conducted this audit to answer the following questions (page 5):

1. Did USAID develop a complete inventory of existing Internet Protocol version 6 compliant devices in accordance with Office of Management and Budget guidance?

2. Did USAID complete an analysis to determine the fiscal and operational impacts and risks of migrating to Internet Protocol version 6 in accordance with Office of Management and Budget guidance?

USAID substantially complied with OMB's memorandum M-05-22 guidance for completing an inventory of network core requirements (page 6) and for completing its impact analysis of migrating to IPv6 (pages 7–8). Furthermore, the Agency plans to conduct and complete its testing of IPv6 with external peers at the Federal Communications Commission and the Department of State prior to OMB's stipulated June 30, 2008, milestone date (page 5).[2] Upon completion of the IPv6 demonstration

[1] Network backbone, similarly denoted as "backbone network," is defined by the Federal Chief Information Officers Council's IPv6 Working Group as the set of network transport devices (e.g., routers, switches) that provide the highest level of traffic aggregation and the highest level of hierarchy in the network. Federal agencies must specify device types, number of devices, and connectivity between devices that constitute their operational core backbone network.

[2] Subsequent to the fieldwork, the Agency notified OMB on June 10, 2008, that it had completed its IPv6 demonstration test through the Internet with external peers in March 2008. The OIG did not review the IPv6 demonstration test results.

tests, the Agency intends to disable IPv6 functionality on its production network backbone but continue testing IPv6 products in a test lab environment (page 8).

The U.S. Government technical requirements and standards representing IPv6 continue to evolve. The National Institute of Standards and Technology is working on its publication "*A Profile for IPv6 in the U.S. Government – Version 1.0*, *Special Publication 500-267 (2nd draft)*" and associated proposed testing program to provide the technical basis upon which long-term U.S. Government IPv6 adoption plans and policies can be based. The profile is not intended for near-term uses (e.g., the June 2008 requirements in M-05-22) but as a forward-looking strategic plan for 2010 and beyond. Additionally, the profile acknowledges that "while significant commercial implementations have and continue to emerge, broad vendor product lines are currently at varying levels of maturity and completeness. Until there is time for significant market forces to effectively define *de facto* standard levels of completeness and correctness, product testing services are likely needed to ensure the confidence and to protect the investment of early IPv6 adopters" (pages 7–8).

However, the testing services and the standards on which testing would be based have not been finalized. In the absence of an IPv6 compliance testing standard, USAID has relied on vendor representations and its own testing efforts for IPv6 capability. USAID has been identifying and replacing non-IPv6 network backbone equipment as part of its multiyear technology refresh program to replace older equipment (page 8).

This audit is not making any recommendations at this time. In response to the draft report, USAID has no comments in regard to the report's findings. USAID's comments are included in their entirety in appendix II of this report (see page 12).

BACKGROUND

Internet Protocol (IP) addresses are a fundamental part of the Internet. Every device connected to the Internet needs an IP address that is represented by a unique number. Currently, two types of IP addresses are in active use worldwide: IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 was initially deployed in January 1983 and is still the most commonly used version in the United States. IPv4 addresses, which are based on 32-bit numbers, can support about 4.3 billion unique addresses. Deployment of the IPv6 protocol began in 1999. IPv6 was developed to address concerns over expected emerging demands for limited IPv4 addresses. IPv6 addresses are based on 128-bit numbers with the capacity to support about 3.4×10^{38} unique addresses. Although differing views exist within the Internet industry as to the pace of demand for the remaining IPv4 addresses, demand for IP addresses is expected to increase as more of the world's population requests Internet access and uses electronic devices that require IP addresses. IPv6 is intended to meet this increased future demand. Consequently, use of both IPv4 and IPv6 is expected to overlap for some time. The hardware and software infrastructure needed to support both IPv4 and IPv6 presents a challenge to the Federal Government.

To guide Federal Government agencies in their transition for IPv6, in August 2005 the Office of Management and Budget (OMB) issued memorandum M-05-22, "*Transition Planning for Internet Protocol Version 6 (IPv6)*," which established the goal for all Federal agency backbone[3] networks to support IPv6 by June 30, 2008. OMB memorandum M-05-22 identifies several key milestones and requirements for all Federal agencies to follow in support of the June 30, 2008, transition date:

By November 15, 2005
- Identify an IPv6 agency lead.
- Complete an inventory of IP-aware devices in its network backbone.

By February 28, 2006
- Develop a network backbone transition plan for IPv6.
- Complete an IPv6 progress report.

By June 30, 2006
- Complete an inventory of IP-aware applications and peripherals with dependencies on its network backbone.
- Complete an IPv6 transition impact analysis.

By June 30, 2008
- Complete network backbone transition to IPv6.

[3] Network backbone, similarly denoted as "backbone network," is defined by the Federal Chief Information Officers Council's IPv6 Working Group as the set of network transport devices (e.g., routers, switches) that provide the highest level of traffic aggregation and the highest level of hierarchy in the network. Federal agencies must specify device types, number of devices, and connectivity between devices that constitute their operational core backbone network.

Additionally, OMB M-05-22 tasked—

- The National Institute of Standards and Technology (NIST) to develop a standard to address IPv6 compliance for the Federal Government,
- The General Services Administration and Federal Acquisition Regulation Council to develop a suitable Federal Acquisition Regulation (FAR) amendment for use by all agencies, and
- The Federal Chief Information Officers Council's (CIOC) Architecture and Infrastructure Committee to develop additional IPv6 transitional guidance for Federal agencies.

In January 2008, NIST issued a second draft for public comment on IPv6 compliance, "*A Profile for IPv6 in the U.S. Government – Version 1.0*, *Special Publication 500-267*." NIST issued its first draft for public comment in February 2007. The General Services Administration, the Department of Defense, and the National Aeronautics and Space Administration issued a notice of a proposed rule in August 2006, FAR Case 2005-041, which would require IPv6-capable products to be included in information technology procurements to the maximum extent possible; however, this proposed rule has not been finalized as of the date of this report. The CIOC has finalized several documents in support of OMB M-05-22 to assist Federal agencies; these include "*IPv6 Transition Guidance*," issued in February 2006, and "*Demonstration Plan to Support Agency IPv6 Compliance*," issued in January 2008.

According to the CIOC's transitional guidance "*Demonstration Plan to Support Agency IPv6 Compliance*," the requirements for June 30, 2008, are for the network backbone (i.e., core) only. IPv6 does not actually have to be operationally enabled by June 30, 2008. However, network backbones must be ready to pass IPv6 traffic and support IPv6 addresses. Agencies are expected to verify this new capability through testing activities and must be able to demonstrate that they can perform *at least* the following functions, without compromising IPv4 capability or network security, by June 30, 2008:

- Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core) to the local area network (LAN).
- Transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers.
- Transmit IPv6 traffic from the LAN, through the network backbone (core), to another LAN (or another node on the same LAN).

For these demonstrations, the CIOC defined a LAN as desktop or laptop personal computers configured to send and receive IPv6 packets and connected to a network backbone with IPv6-enabled networking equipment. External networks can belong to another agency, an Internet service provider, or another organization capable of transmitting IPv6 traffic. The testing of other information technology assets (e.g., applications) is not required for the June deadline.

USAID plans to conduct and complete its testing of IPv6 on its network backbone with the Federal Communications Commission and the Department of State prior to OMB's stipulated June 30, 2008, deadline.

AUDIT OBJECTIVES

The Office of Inspector General, Information Technology and Special Audits Division, included this audit in its fiscal year 2007 audit plan to answer the following questions:

1. Did USAID develop a complete inventory of existing Internet Protocol version 6 compliant devices in accordance with Office of Management and Budget guidance?

2. Did USAID complete an analysis to determine the fiscal and operational impacts and risks of migrating to Internet Protocol version 6 in accordance with Office of Management and Budget guidance?

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

AUDIT FINDINGS

Did USAID develop a complete inventory of existing Internet Protocol version 6 compliant devices in accordance with Office of Management and Budget guidance?

USAID substantially complied with the Office of Management and Budget's (OMB) memorandum M-05-22 to prepare a complete inventory of network backbone devices.

Overall, USAID has been responsive to OMB's Internet Protocol version 6 (IPv6) inventory requirements. The Agency developed an initial inventory of its network backbone in November 2005 and an updated listing in June 2006 that totaled about 715 items of equipment. USAID subsequently revised its inventory of IPv6 network backbone equipment in November 2007 as a result of newer guidance issued by the Federal Chief Information Officers Council (CIOC) that defined a "network backbone" (i.e., core network) for use by executive agencies in support of OMB M-05-22. As a result of this definitional clarification, USAID's inventory was reduced to 24 items of equipment, which represented the Agency's metropolitan area network (MAN)[4] as its network backbone. The audit team's verification of the Agency's inventory list identified two more pieces of equipment that were not on the Agency's inventory of 24 items. The two additional pieces of equipment were determined to be part of the Agency's network backbone that provided redundancy to maintain availability. Although two items were not included in the Agency's list, the omission was not considered material. Agency officials indicated that the two items were added after submitting their inventory listing to OMB.

[4] A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region. The term is applied to the interconnection of networks in a city into a larger network.

Did USAID complete an analysis to determine the fiscal and operational impacts and risks of migrating to Internet Protocol version 6 in accordance with Office of Management and Budget guidance?

USAID substantially complied with OMB's guidance to complete its analysis of fiscal and operational impacts and risks of migrating to Internet Protocol version 6.

OMB memorandum M-05-22 required agencies to complete an IPv6 transition impact analysis by June 30, 2006, with the goal of completing a demonstration test of their network backbone for IPv6 by June 30, 2008. The USAID lead person responsible for the Agency's transition to IPv6 stated that the transition impact analysis for IPv6 was completed within OMB's June 30, 2006, milestone date. A copy of USAID's impact analysis was obtained and reviewed. Based on this review, it was found that USAID—

- Completed an IPv6 transition impact analysis as required.
- Identified key concerns and some possible solutions.
- Prepared a cost budget addendum to support the impact analysis.

USAID's impact analysis identified risks that included security, investment funding, immature technology, and operational issues for managing an IPv6 network. It also provided mitigating approaches to reduce some of the identified risks. The Agency proposed solutions to address some of the risks that were based on assumptions developed prior to the June 2006 OMB milestone date. Among the concerns that the Agency identified in its impact analysis were the following information security and training risks:

- Information Security – The new protocol [IPv6] is a significant change in how networks transport information. All existing tools, along with relative policies and procedures, need to be evaluated to see if they can provide the same functionality or if they need to be modified, replaced, or augmented…and that USAID needs to provide the same or greater protection in the IPv6 environment as is in place for IPv4.
- Training – The security operations staff would need training and additional tools to be able to identify IPv6 traffic for the types of vulnerabilities they protect against now using IPv4. Additionally, the Agency would need to develop a training plan for the various operating groups [formerly IRM Operations] within the Office of the Chief Information Officer.

The risks identified in the Agency's impact analysis are not considered to be urgent concerns that require immediate attention because the Agency's network has not transitioned to IPv6. However, the concerns are significant issues to be considered when supporting a network transitioning to IPv6. In its impact analysis, the Agency recognized that some risks could not be addressed based on the technological maturity of available products, technical standards, and specifications existing at that time.

As of May 2008, there still was no immediate urgency for the Agency to adopt IPv6, particularly when IPv6 standards and technical requirements for the U.S. Government continue to evolve. The U.S. Government, however, continues to make progress in

addressing the IPv6 challenge by developing technical standards, specifications, and testing programs.

For example, the NIST publication "*A Profile for IPv6 in the U.S. Government – Version 1.0*, *Special Publication 500-267 (2nd draft)*" and its associated proposed testing program are to provide the technical basis upon which long-term U.S. Government IPv6 adoption plans and policies can be based. The profile is not intended for near-term uses (e.g., the June 2008 requirements described in M-05-22). Instead, as a forward-looking strategic plan, the profile's recommendations are targeted for 2010 and beyond. Additionally, the NIST publication states that "while significant commercial implementations have and continue to emerge, broad vendor product lines are currently at varying levels of maturity and completeness. Until there is time for significant market forces to effectively define *de facto* standard levels of completeness and correctness, product testing services are likely needed to ensure the confidence and to protect the investment of early IPv6 adopters."

Because testing services and standards have not been finalized, USAID officials indicated that they have relied on vendor representations and the Agency's own testing for IPv6 capability. USAID has been identifying and replacing non-IPv6 network backbone equipment as part of its multiyear technology refresh program to replace older equipment. The Agency plans to disable IPv6 on its production network (i.e., outside a test lab environment) after its IPv6 demonstration test to OMB.[5]

However, USAID's management provided comments that the Agency will continue to test products supporting IPv6 and update how it would address identified risks in its impact analysis beyond June 2008 on the basis of research and testing.

[5] Subsequent to the fieldwork, the Agency notified OMB on June 10, 2008, that it had completed its IPv6 demonstration test through the Internet with external peers in March 2008. The OIG did not review the IPv6 demonstration test results.

EVALUATION OF MANAGEMENT COMMENTS

In its response to the draft report, USAID did not have any comments regarding the findings. USAID's comments from the Office of the Chief Information Officer are included in appendix II.

SCOPE AND METHODOLOGY

Scope

The Office of Inspector General, Information Technology and Special Audits Division, performed this audit to determine whether USAID developed, in accordance with Office of Management and Budget (OMB) guidance, (1) a complete inventory of existing Internet Protocol version 6 (IPv6) compliant devices and (2) a complete analysis of fiscal and operational impacts and risks of migrating to IPv6.

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

Audit fieldwork was conducted between November 2007 and May 2008, primarily at USAID headquarters in Washington, DC; the Tech Hub in Rosslyn, VA; and the Beltsville Information Management Center and the Teleport Center in Laurel, MD. The audit team met several times with the IPv6 project team lead and USAID technical and network experts associated with the project.

In support of our audit objectives, we evaluated the Agency's actions and responses to OMB memorandum M-05-22 requirements and milestones for transitioning from IPv4 to IPv6. Specifically, we evaluated whether the Agency—

By November 15, 2005
- Completed an inventory of IP-aware devices in its network backbone.

By June 30, 2006
- Completed an inventory of IP-aware applications and peripherals with dependencies on its network backbone.
- Completed an IPv6 transition impact analysis.

By June 30, 2008
- Is on target to complete its network backbone transition to IPv6.

The audit reviewed interpretive documentation issued by the Federal Chief Information Officers Council's (CIOC) Architecture and Infrastructure's IPv6 Working Group, proposed Federal Acquisition Regulations for IPv6, and the National Institute of Standards and Technology's (NIST) "*A Profile for IPv6 in the U.S. Government – Version 1.0*, *Special Publication 500-267*," in support of OMB M-05-22. We also obtained and reviewed a joint publication issued by NIST and the National Telecommunications and Information Administration, titled "*Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)*," dated January 2006.

We also included in our scope the control procedures for the disposal and surplus of excess equipment to ensure that any nonvolatile memory or other data storage

component within the Agency's network backbone was effectively erased upon device disposal or surplus. Additionally, OMB, through guidance issued by the CIOC, required demonstration of IPv6 network backbone compliance for the June 30, 2008, milestone by having executive agencies perform specific tests and document the results. Consequently, we obtained and reviewed documentation on the IPv6 test procedures and applicable test results that were performed in 2007 by USAID engineers and systems contractors to show support for the Agency's compliance. At the start of this audit, the Agency had not yet completed its demonstration tests through the Internet with external peers; however, the Agency planned to complete these tests prior to June 30, 2008. Subsequent to our fieldwork, the Agency notified OMB on June 10, 2008, that it had completed its IPv6 demonstration test through the Internet with external peers in March 2008. We did not review the March 2008 IPv6 test results.

Methodology

For the first audit objective, we obtained and reviewed the Agency's inventory list of existing network backbone devices that represented its metropolitan area network (MAN). To determine the accuracy and completeness of the Agency's network backbone inventory listing, we (1) traced all 24 items on the inventory list to their physical locations and (2) traced equipment items at their physical locations that were identified by Agency engineers as belonging to the network backbone (i.e., MAN) to the equipment inventory list. For the purposes of this test, we established a 10 percent materiality threshold, which meant that three or more items identified as deficient would be deemed material.

For the second audit objective, we obtained a copy of the Agency's impact analysis to determine whether it was completed. We interviewed the Agency IPv6 project lead to learn how the analysis was prepared and reviewed, and discussed the strategy for mitigating risks and concerns identified in the Agency's impact analysis. We reviewed guidance issued by the CIOC to identify some of the elements that may be considered in an agency's impact analysis for migrating to IPv6. Based on our review of the potential elements that could be represented in an impact analysis and the content of the Agency's impact analysis, we subjectively concluded that the analysis was substantially complete for meeting and addressing risks associated with the June 30, 2008, network backbone demonstration test.

MANAGEMENT COMMENTS

August 20, 2008

MEMORANDUM

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

FROM: M/CIO, Phil Heneghan /s/

SUBJECT: Draft Audit of USAID's Implementation of Internet Protocol Version 6 (Audit Report No. A-000-08-XXX-P)

Thank you for the opportunity to comment on the Draft Audit of USAID's Implementation of Internet Protocol Version 6 (Audit Report No. A-000-08-XXX-P)

After extensive review, the Office of the Chief Information Officer has no comments on the Findings.

Please accept my thanks for the cooperation and courtesies extended to my staff duing this audit by members of your office.

Cc: Carl Crawford
Gretchen Larrimer

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