USAID
FROM THE AMERICAN PEOPLE

OFFICE OF INSPECTOR GENERAL

AUDIT OF USAID'S IMPLEMENTATION OF SELECTED HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 REQUIREMENTS FOR PERSONAL IDENTITY VERIFICATION OF FEDERAL EMPLOYEES AND CONTRACTORS

AUDIT REPORT NO. A-000-08-004-P
February 06, 2008

WASHINGTON, DC

Office of Inspector General

February 06, 2008

MEMORANDUM

TO: CIO/M, Chief Information Officer, David C. Anewalt

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

SUBJECT: Audit of USAID's Implementation of Selected Homeland Security Presidential Directive 12 (HSPD-12) Requirements for Personal Identity Verification of Federal Employees and Contractors (Audit Report No. A-000-08-004-P)

This memorandum transmits the Office of Inspector General's final report on the subject audit. 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.

The report contains one recommendation. Based on your response to our draft report, we have reached a management decision on the recommendation. Please notify the Bureau for Management's Audit, Performance and Compliance Division when final action is completed.

I appreciate the cooperation and courtesies extended to my staff during this audit.

cc: Office of Security, Randy Streufert

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

CONTENTS

SUMMARY OF RESULTS

Homeland Security Presidential Directive 12 (HSPD-12) requires the development and implementation of a mandatory Governmentwide standard for secure and reliable forms of identification of Federal employees and contractors to access federally controlled facilities and information systems. The Office of Inspector General, Information Technology and Special Audits Division, in Washington, DC, conducted an audit to determine whether USAID addressed selected HSPD-12 requirements[1] from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) in support of Personal Identity Verification (PIV) of Federal employees and contractors. The audit assessed USAID's progress on selected HSPD-12 requirements and milestones due in calendar years 2007 and 2008 (see page 5).

In support of HSPD-12, OMB outlined the implementation schedule to executive agencies. Selected HSPD-12 requirements will be addressed in two phases that incorporate the use of various NIST technical requirements. PIV-I requires agencies to develop policies and procedures to verify the personal identities of Federal employees and contractors, including identity verification for applicants, background checks, and employee registration. PIV-II defines the technical requirements and functions that agencies must incorporate into a Federal identity credential. During PIV-II, agencies must demonstrate their ability to issue new identification cards to all employees and contractors. Employees and contractors who started Federal employment since October 2005 are required to follow PIV-I requirements for identity verification. Employees and contractors who started Federal employment since October 2006 are required to meet PIV-I requirements and receive identity credentials that conform to PIV-II requirements. Current employees and contractors who started their employment prior to October 2005 are required to have complete background checks by October 2007 or October 2008, depending on their years of service (see page 4).

USAID's Office of Security had implemented policies and procedures before the HSPD-12 initiative to ensure that USAID employees, contractors, and other Government personnel had adequate background checks or underwent personal security investigations and vetting. However, the audit found that USAID did not fully address selected HSPD-12 requirements from the Office of Management and Budget and National Institute of Standards and Technology in support of Personal Identity Verification. Specifically, USAID did not fully comply with PIV-I requirements because USAID personnel could not identify or retrieve all of the identity proofing documents from the Department of State's (DoS) Identity Management System. USAID also did not meet the OMB PIV-II target date to issue new Federal identity credentials to current employees and contractors in 2007, nor will it meet OMB's 2008 target date based on prior rates of issuance (see page 6). Several factors contributed to USAID's inability to meet the PIV-I and PIV-II requirements: (1) USAID's lack of an implementation plan as required by OMB, (2) USAID's decision not to establish HSPD-12 as a higher-priority information technology (IT) investment, (3) USAID's dependence on DoS implementation of HSPD-12, (4) NIST's evolving technical requirements, and (5) OMB's funding constraint on Agency budget requests. Some of these factors were external to USAID and thus outside of USAID's control.

[1] The requirements selected were based on OMB's HSPD-12 implementing instructions and are shown in table 1 on page 4 of this report.

Nonetheless, without a plan to implement HSPD-12 and Agency support to fund HSPD-12 as a higher-priority IT investment, USAID's project managers are left with few or no details about how they can best implement HSPD-12. As a result, project managers made ad hoc decisions regarding funding, resources, and technical approaches that may not have been realistic and ultimately may have delayed or prevented the Agency's implementation of this Governmentwide mandate. If USAID does not implement PIV-I and PIV-II, it may not fully realize the critically needed security benefits of PIV, and interoperability among Federal agency PIV card programs (one of the major goals of HSPD-12) may not be achieved (see pages 7–11).

This report makes one recommendation to improve USAID's implementation of HSPD-12 (see page 11). In response to the draft report, USAID agreed with the audit recommendation, outlined its plans to address the audit recommendation, and provided estimated dates when the final action would be completed. Based on an evaluation of the Agency's comments, a management decision has been reached on the recommendation (see page 12). USAID's comments are included in their entirety in appendix II of this report (see page 15).

BACKGROUND

In response to terrorist attacks on the United States, the President issued a series of initiatives to increase security across Government agencies. On August 27, 2004, the President signed Homeland Security Presidential Directive 12 (HSPD-12), which required the development and implementation of a mandatory Governmentwide standard for secure and reliable forms of identification to allow Federal employees and contractors to gain physical access to federally controlled facilities and logical access to federally controlled information systems. The goals of HSPD-12 emphasized security and interoperability among Federal Government agencies and specified that identity credentials would be—

- Issued based on firm criteria to verify an employee's identity;
- Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Rapidly authenticated electronically; and
- Issued only by providers whose reliability had been established.

HSPD-12 assigns responsibility to the Office of Management and Budget (OMB) for overseeing executive agencies' implementation of HSPD-12 and to the National Institute of Standards and Technology (NIST) for issuing technical guidance. NIST issued Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, and other supporting technical publications to help executive agencies implement HSPD-12's requirements.

In August 2005, OMB issued memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, to executive branch agencies with instructions and timeframes to implement selected HSPD-12 requirements. OMB and NIST defined HSPD-12's implementation in two phases: PIV part one (PIV-I) and PIV part two (PIV-II). Table 1 summarizes some selected key OMB requirements and timeframes to implement selected requirements under PIV-I and PIV-II.

Table 1. HSPD-12 Selected Requirements and OMB Implementation Deadlines[2]

HSPD-12 Selected Requirements	OMB Implementation Deadlines
PIV-I	
1. Initiate national agency check with inquiry (NACI) before credential issuance	10/27/05
2. Maintain and identify the two types of documents used for employee and contractor identity proofing	10/27/05
3. Complete background investigations for current employees and contractors with fewer than 15 years of service	10/27/07
4. Complete background investigations for current employees and contractors with more than 15 years of service	10/27/08
PIV-II	
5. Start issuance of identity credentials	10/27/06
6. Issue and require the use of identity credentials for current employees and contractors with fewer than 15 years of service	10/27/07
7. Issue and require the use of identity credentials for current employees and contractors with more than 15 years of service	10/27/08
8. Use the credentials' electronic security features to authenticate identities to gain physical access to facilities	*
9. Use the credentials' electronic security features to authenticate identities to gain electronic access to information systems	*

*According to OMB's HSPD-12 implementation guidance, agencies are not required to complete implementation of all card capabilities on October 27, 2006. Thus, agencies are not expected to have their entire infrastructure installed to enable use of the cards at all facilities and systems. However, agencies are expected to make use of the cards using a risk-based approach.

PIV-I requires agencies to develop policies and perform specific procedures to ensure that the personal identities of employees and contractors are verified and registered before issuing Federal identity credentials. During identity proofing, the applicant is required to provide two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, *OMB No. 1115-0136, Employment Eligibility Verification*, and at least one of the documents must be a valid State or Federal government-issued picture identification. Additionally, the identity source documents used for identity proofing must be recorded by the Agency. PIV-II provides guidance on technical interoperability requirements, implementation, issuance, and use of identity credentials. Current employees and contractors who started their employment prior to October 27, 2005, were required to have complete background checks by October 27, 2007, or October 27, 2008, depending on their years of service. However, new employees and contractors who started employment since October 27, 2005, were immediately subject to PIV-I background check requirements for identity verification. New employees and contractors who started employment since October 27, 2006, were immediately subject to both PIV-I and PIV-II requirements.

[2] Source: Office of Management and Budget, Memorandum M-05-24, dated August 5, 2005.

When PIV-II is fully implemented Governmentwide, the holder of an identity credential card from one agency can be electronically authorized by another agency to access its facilities and systems. The identity credentials store encoded data on a credit card–sized card that verifies the identity of each cardholder through a card reader. For example, a cardholder presents the credential to a card reader at a physical entrance to request access to a Federal Government facility. Once the data are read, the card reader sends the information to an access control system that will either grant or deny access to the cardholder. Similarly, when a cardholder presents the credential to a card reader for network access at a login screen, the logical access control system validates the cardholder's credential and authenticates the identity of the cardholder before granting access to an information technology (IT) system.

USAID's implementation of HSPD-12 is led by personnel within USAID's Office of the Chief Information Officer (CIO) and Office of Security (SEC). USAID's Acting CIO was tasked to design, develop, implement, and maintain security access systems, including security identification and credentialing for USAID employees and contractors. Under USAID's Office of the CIO, the Chief Information Security Office was responsible for registering the enrollment of personnel into the identity management system used to issue credentials. USAID's SEC was responsible for ensuring that USAID employees, contractors, and other Government personnel had or followed appropriate personal security background checks. SEC was responsible for credential issuance, maintenance, and security for physical access to USAID headquarters.

To support the HSPD-12 project, USAID's SEC entered into a 5-year memorandum of understanding with the Bureau of Diplomatic Security within the Department of State (DoS). This interagency agreement enrolled USAID in the DoS Identity Management System (IDMS), which enabled USAID to issue and renew credentials based on DoS PIV-II cards.

DoS is responsible for issuing credentials to USAID employees and contractors assigned to overseas posts. As of May 2007, approximately two-thirds of USAID's total workforce was assigned to overseas posts, with the remaining third located at U.S. headquarters.

As of April 2007, USAID's HSPD-12 project team had obligated about $251,000 for the purchase of equipment and contractor support to implement HSPD-12.[3]

AUDIT OBJECTIVE

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 question:

> Did USAID address selected requirements from the Office of Management and Budget and the National Institute of Standards and Technology in support of Homeland Security Presidential Directive 12 for Personal Identity Verification of Federal Employees and Contractors?

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

[3] The Office of the CIO and the Office of Security provided approximately $110,000 and $141,000, respectively.

AUDIT FINDING

As shown in table 2 below, USAID did not fully address selected HSPD-12 requirements from the Office of Management and Budget and National Institute of Standards and Technology in support of Personal Identity Verification.

Table 2. HSPD-12 Selected Requirements, OMB Deadlines and Status of USAID's Planned Completion Dates (as of May 31, 2007)

Selected HSPD-12 Requirements	OMB Deadline	USAID's Completion Date	Has USAID Met Requirement?
Compliance with PIV-I[4]			
1. Initiate national agency check with inquiry (NACI) investigations prior to credential issuance or alternate check	10/27/05	10/26/05	Yes
2. Maintain and identify the two types of documents used for employee and contractor identity proofing	10/27/05	To Be Determined (TBD)	No*
3. Complete background investigations for current employees and contractors with fewer than 15 years of service	10/27/07	10/26/05	Yes
4. Complete background investigations for current employees with more than 15 years of service	10/27/08	10/26/05	Yes
Compliance with PIV-II			
5. Start issuance of identity credentials	10/27/06	10/27/06	Yes
6. Issue and require the use of identity credentials for current employees and contractors with fewer than 15 years of service	10/27/07	TBD	No (Estimate ~ 2011 or later)
7. Issue and require the use of identity credentials for current employees and contractors employed with more than 15 years of service	10/27/08	TBD	No (Estimate ~2011 or later)
8. Use the credentials' electronic security features to authenticate identities to gain physical access to facilities	**	TBD	No***

[4] As required, USAID recognized federally awarded clearances performed by other U.S. Government agencies.

(Table 2 – *continued from previous page*)

9. Use the credentials' electronic security features to authenticate identities to gain electronic access to information systems	**	TBD	No***

* USAID could neither identify nor retrieve from the Identity Management System the two forms of identification used to vet an individual's identity that were issued a Federal identity credential as required by NIST 201 for 9 out of 20 sampled employees.
** According to OMB's HSPD-12 implementation guidance, agencies are not required to complete implementation of all card capabilities on October 27, 2006. Thus, agencies are not expected to have their entire infrastructure installed to enable use of the cards at all facilities and systems. However, agencies are expected to make use of the cards using a risk-based approach.
*** USAID did not develop an implementation plan that included estimated due dates for meeting these requirements.

Implementation Plan Is Needed for HSPD-12

Summary: USAID did not fully comply with PIV-I requirements because USAID personnel could not identify or retrieve all of the identity proofing documents from the Department of State's (DoS) Identity Management System. USAID also did not meet the OMB PIV-II target date to issue new Federal identity credentials to current employees and contractors in 2007, nor will it meet OMB's 2008 target date based on prior rates of issuance. USAID did not meet the above-noted requirements in OMB Memorandum M-05-24 and supporting documents, in part because it did not (1) develop an implementation plan in support of HSPD-12 or (2) establish HSPD-12 as a higher-priority IT investment. As a result, USAID project managers who are responsible for issuing and meeting OMB Federal identity credential deadlines and the requirement to use the Federal identity credential to access Federal facilities and information systems had few or no details as to how they could best implement these requirements in concert with DoS. This led to project managers having to make ad hoc decisions regarding funding, resources, and technical approaches that may not have been realistic and ultimately may have delayed or prevented the Agency's implementation of this Governmentwide mandate. Therefore, USAID may not fully realize the critically needed security benefits of PIV, and more important, interoperability among Federal agency PIV card programs (one of the major goals of HSPD-12) may not be achieved.

As shown in table 2, USAID did not fully comply with PIV-I requirements for credentials issued under PIV-II. OMB memorandum M-05-24 directs that PIV-I identity proofing and registration processes must be consistent with NIST guidance and applied to all new identity credentials. This includes the PIV-I requirement to identify or retrieve the two source documents presented for identity proofing of employees and contractors. The two documents must come from the list of acceptable documents included in Form I-9, *OMB No. 1115-0136, Employment Eligibility Verification*.

Neither Department of State nor USAID could identify or retrieve from the identity management system used by USAID and maintained by the Department of State the two identity source documents used for 9 out of 20 sampled employees. Nor did USAID have any other records to provide this information to the OIG when requested. Consequently, USAID could not demonstrate its compliance with the PIV-I requirement. When USAID's project manager was made aware of this problem, the project manager promptly communicated it to USAID's Office of Security and Department of State for resolution. Because USAID is taking steps to address this issue, the Office of Inspector General is not making a formal recommendation to address this problem at this time.

USAID also did not meet OMB's 2007 PIV-II target date to issue and use identity credentials for employees and contractors with fewer than 15 years of service, and will not meet OMB's 2008 target date to issue new identity credentials to current employees and contractors with more than 15 years, based on prior rates of issuance. USAID began issuing PIV-II credentials in October 2006. From October 2006 through May 2007, USAID issued 497 credentials to its approximately 3,100 employees and contractors at headquarters. This equates to roughly 60 credentials per month. At this rate of issuance, USAID would need more than 3 years to issue credentials for the approximately 2,600 remaining employees and contractors at headquarters. Consequently, USAID did not meet OMB's October 2007 and based on these rates of issuance will not meet OMB's 2008 target dates. USAID's HSPD-12 project team members indicated that resource constraints limited the number of credentials that could be issued.

Further, USAID officials from the Office of the CIO and the SEC acknowledged that they could not meet OMB's PIV-II target dates of October 2007 and 2008 for issuance and to start using the credentials' electronic features to authenticate cardholder identities to access facilities and information systems.

More important, USAID will not meet the PIV-II requirements because it did not develop an implementation plan. An implementation plan would serve as the Agency's road map to provide action-oriented direction in defining key milestones, processes, and specifications to implement the logical and physical access requirements of HSPD-12. Additionally, it would provide a concept of operation and identify the resources required to support the implementation of HSPD-12's PIV-II requirements. According to OMB's instructions for implementing HSPD-12, agencies were required to submit their implementation plans to OMB by June 27, 2005.

Although USAID did not prepare an implementation plan for OMB that described a comprehensive strategy, the HSPD-12 project team has tried to develop an approach to implement PIV-II and has modified its approach several times since the beginning of the HSPD-12 initiative.

The Agency's initial approach started with the development of a business case[5] in the fall of 2005 for funding in the FY 2007 budget cycle. The project team estimated that about $17 million would be required to implement HSPD-12 at headquarters and at 60 overseas missions worldwide. The business case's acquisition plans presumed that USAID would purchase its own Identity Management System (IDMS). In this approach, the acquisition plans assumed no DoS participation. USAID officials indicated that this initial approach was changed due to funding limitations in the spring of 2006, when the Agency sought to enter into an interagency service agreement with DoS. Under this agreement, DoS would be responsible for producing and issuing identity credentials for USAID employees and contractors. This draft agreement was never formalized and subsequently changed.

Nonetheless, USAID entered into a signed agreement to use the DoS IDMS. USAID would obtain PIV-II cards from DoS and issue the PIV-II cards as Federal identity credentials to USAID headquarters' employees and contractors. However, the project team officials indicated that DoS would not allow USAID's facility and IT systems to be connected to its

[5] A business case is a formal document used to evaluate and justify IT project investment requests from either the capital investment or operating expense funds.

IDMS. Therefore, the agreement with DoS alone will not address the technical requirements and functions to access facilities and IT systems that USAID must incorporate to use the Federal identity credential.

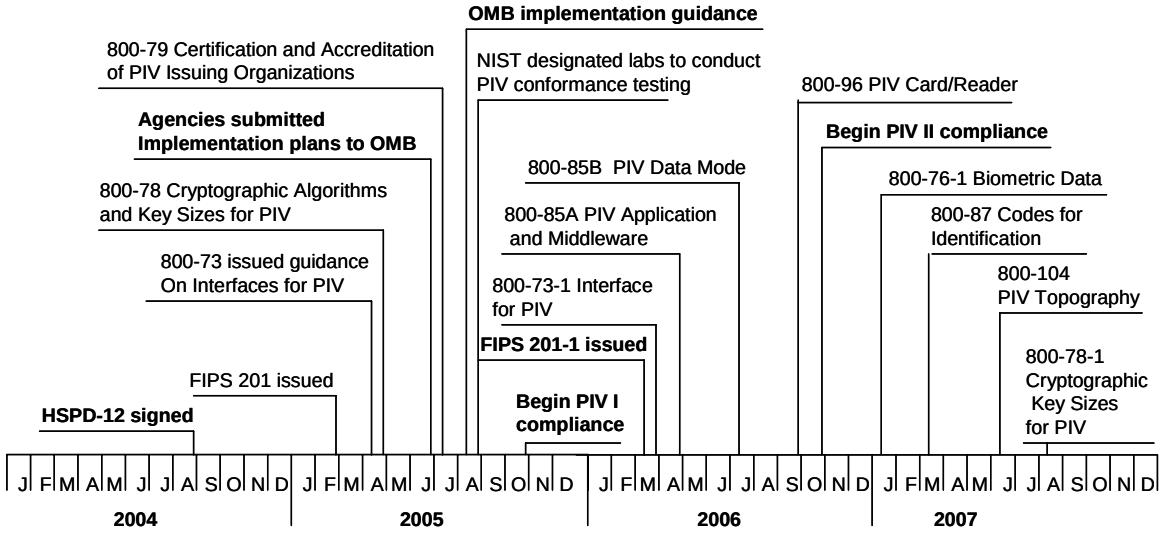
Under the current approach, three functional components operate independently: (1) IDMS, the DoS system that USAID is using to issue and renew PIV identity credentials; (2) a system that assigns access privileges for employees and contractors to access USAID's facilities; and (3) systems that authenticate access privileges for employees and contractors to specific information systems. Even though OMB's implementation guidance directs agencies to phase in the use of the Federal identity credential capabilities at facilities and systems, USAID's project team has not addressed how the use of the Federal identity credentials will be phased in to integrate these functional components into a single credential. Specifically, USAID did not develop an implementation plan that addressed the integration of these functional components.

Additionally, USAID's HSPD-12 project team members indicated that USAID will not meet the PIV-II requirements because of funding constraints. Project managers for HSPD-12 indicated that the Agency did not restructure its major IT investments to provide additional resources to support this Governmentwide initiative because of other competing Agency projects that needed funding.

Despite the lack of total funding for HSPD-12, as of April 2007 the project team had obtained $251,000 from the offices of the Chief Information Officer and Office of Security to support the HSPD-12 project, which included the service agreement with DoS, contractor support, and equipment purchases used to enroll applicants and issue credentials. Subsequent to the OIG's fieldwork, the Agency provided additional funds for fiscal years 2008 and 2009. Therefore, the Office of Inspector General is not making a recommendation regarding the project's funding.

During the audit, three external factors were also identified as reasons USAID had not met the PIV-II requirements. First, USAID's employees and contractors working in overseas posts rely on DoS regional security officers for identity credentials; however, PIV-II identity credentials cannot be issued until DoS deploys its new credentials to its overseas posts. As of May 2007, DoS estimated that deployment of its new credentials will not be completed until 2011 or later—at a minimum, more than 3 years past OMB's schedule. Second, NIST continued to issue various technical requirements after OMB issued its implementing instructions to executive agencies. For example, several months before and after agencies were to start compliance with PIV-II in October 2006, key publications needed to implement the technical requirement provisions of FIPS 201 were revised and reissued. Thus, agencies did not have sufficient time to test and acquire compliant products within OMB required timeframes. Figure 1 on the next page illustrates when NIST issued FIPS 201 and subsequent technical publications and guidance in relation to the signing of HSPD-12 and OMB's instructions to agencies.

Figure 1. Time Line of FIPS 201 and Related Activities (as of August 2007)



Third, OMB initially announced to agencies that no additional funding would be provided to implement the requirements of HSPD-12. OMB expected agencies to fund HSPD-12 through existing funds. OMB anticipated that agencies would restructure their major investments to pay for HSPD-12. Moreover, because all Federal agencies have existing background investigation, access control, and identification credential activities, OMB anticipated that these activities, and the funding used to support them, would be used to support HSPD-12 activities.

Although these factors are external to USAID and important, the Office of Inspector General is not making any recommendations to address them in this report.

CONCLUSION

Although some challenges and dependencies remain outside USAID's control and prevent it from addressing and obtaining full compliance with PIV-I and PIV-II requirements within OMB's stipulated completion target dates, USAID can make improvements, such as developing a plan, to advance the implementation of HSPD-12. Without an implementation plan, project managers who are responsible for implementing the physical and logical access requirements mandated in PIV-II are left with few or no details about how they can best implement these requirements in concert with the DoS IDMS system. This situation leads project managers to make ad hoc decisions regarding funding, resources, and technical approaches that may not be realistic and may delay or prevent the Agency's implementation of this Governmentwide mandate. Furthermore, the critical security benefits of PIV may not be fully realized, and more important, interoperability among Federal agency PIV card programs (one of the major goals of HSPD-12) may not be achieved. Consequently, USAID needs to define required resources and plan how it will implement PIV-II, including issuance of credentials to support physical and logical access to USAID facilities and systems.

Therefore, the Office of Inspector General is making one recommendation to assist the Agency's implementation of HSPD-12:

Recommendation No. 1: We recommend that USAID's Chief Information Officer develop and document an implementation plan for Personal Identity Verification Part II, and submit the plan to the Office of Management and Budget.

EVALUATION OF MANAGEMENT COMMENTS

In its response to the draft report, USAID agreed with the audit finding and the one recommendation made in the report. The Agency outlined its plans to address the audit recommendation and provided corrective action plans and target completion dates. As a result, management decisions have been reached for recommendation no. 1.

USAID provided additional comments that were considered when finalizing this audit report. To clarify the information in tables 1 and 2 from the draft report, item numbers 2 and 4 were added (i.e., "Identify and maintain the two types of documents…" and "Start issuance of identity credentials"). In addition, the recommendation was modified by deleting the following second sentence: "*In developing this plan, consideration should be given to explore other options to implement Homeland Security Presidential Directive 12*."

USAID's consolidated comments, which incorporate comments from the Office of the Chief Information Officer and the Office of Security, are included in appendix II.

SCOPE AND METHODOLOGY

Scope

This audit was performed in accordance with generally accepted Government auditing standards. The Office of Inspector General, Information Technology and Special Audits Division performed this audit to determine whether USAID addressed selected requirements of the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) in implementing Homeland Security Presidential Directive 12 (HSPD-12) for Personal Identity Verification (PIV) of Federal employees and contractors.

Audit fieldwork was conducted between January and August 2007, primarily at USAID headquarters in Washington, DC, and in Northern Virginia. The audit team met with Department of State (DoS) Diplomatic Security personnel and visited their data processing facility in Northern Virginia, which supports the IDMS system that USAID uses.

In support of the audit objective, the audit team evaluated internal controls related to the implementation of PIV-I and PIV-II requirements. The scope of work focused on USAID headquarters employees and contractors, and covered the following areas:

- Personal identity proofing processes
- Memorandum of understanding between DoS and USAID for access and use of IDMS assets
- Federal identity credential issuance processes
- HSPD-12 implementation planning
- HSPD-12 information technology project prioritization and budgeting

The audit team evaluated whether the HSPD-12 project team had documented plans to phase in the use of Federal identity credentials to access Federal facilities and information systems to meet selected OMB and NIST requirements and deadlines for selected HSPD-12 requirements (see methodology section below).

As of April 2007, USAID's HSPD-12 project team had obligated nearly $251,000 for the purchase of equipment and contractor support to implement HSPD-12.

Methodology

As the framework for designing this audit, the audit team identified requirements primarily from HSPD-12, OMB's HSPD-12 implementation instructions issued in August 2005,[6] and NIST's Federal Information Processing Standards (FIPS) 201. From these documents, the team judgmentally selected nine key requirements as a basis for evaluating USAID's progress for implementing HSPD-12. They included four requirements within PIV-I and five requirements within PIV-II. PIV-I selected requirements were (1) initiate national agency check with inquiry (NACI) investigations before credential issuance or alternate check, (2) maintain and identify the two types of documents used for employee and

[6] OMB Memorandum, M-05-24.

contractor identity proofing, (3) complete background investigations for all current employees and contractors with fewer than 15 years of service, and (4) complete background investigations for current employees and contractors with more than 15 years of service. PIV-II selected requirements were (1) issue identity credentials, (2) issue and require the use of identity credentials for all current employees and contractors with fewer than 15 years of service, (3) issue and require the use of identity credentials for all current employees and contractors with more than 15 years of service, (4) use the credentials' electronic security features to authenticate identities to gain physical access to facilities, and (5) use the credentials' electronic security features to authenticate identities to gain electronic access to information systems.

The audit team evaluated whether each of the nine selected requirements was met on the basis of HSPD-12, OMB, and NIST completion target dates and requirements. Additionally, for requirements for which the completion target dates have not yet passed and which are likely not to be met, the team evaluated whether documentation (such as implementation plans and rates of credential issuance) existed to determine whether requirements could be completed by the target date. In reviewing the rates of credential issuance, the team assumed a constant rate based on historic rates of issuance and projected that rate to future periods to determine whether the target could be met.

The audit team reviewed a prior Government Accountability Office (GAO) audit report, *Agencies Face Challenges in Implementing New Federal Employee Identification Standard* (dated February 2006); the Federal Identity Credentialing Committee's *Federal Identity Management Handbook*; and applicable USAID documentation relating to planning, budgeting, and implementation of HSPD-12 requirements. The team met with USAID project team members from the Office of the Chief Information Officer and the Office of Security. The team conducted a walk-through of the DoS facility housing the Identity Management System servers and met with DoS staff involved with server administration as well as DoS contacts used by USAID for HSPD-12 support efforts.

To test whether PIV-I and PIV-II procedure requirements were implemented to meet OMB's and NIST's FIPS 201 requirements, the audit team judgmentally selected a total of 20 direct hire and contractor staff working at headquarters[7] who were issued new identity credentials between October 27, 2006, and January 24, 2007. The team tested four attributes to determine whether the following steps were completed:

- Two forms of ID were on file.
- Background investigations were completed (including adjudication).
- Federal Bureau of Investigation fingerprint check was completed and one fingerprint card was on file.
- Signed USAID form 500-1 (authorizing logical and physical access) was on file.

In addition, the audit team tested management control processes associated with the receipt, issuance, and storage of PIV-II cards. Owing to the importance of the vetting process, our noncompliance materiality threshold was set to one.

[7] Out of the 30 judgmentally selected direct hires and contractors, 20 were issued PIV cards and 10 were issued Facility Access Cards.

MANAGEMENT COMMENTS

December 10, 2007

MEMORANDUM

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

FROM: M/CIO, David Anewalt /s/

SUBJECT: Audit of USAID's Implementation of Selected Homeland Security Presidential Directive 12 (HSPD-12) Requirements for Personal Identity Verification of Federal Employees and Contractors (Audit Report No. A-000-08-00X-P)

Thank you for the opportunity to respond to the draft audit report. This memorandum contains the management decision for the draft Audit of USAID's Implementation of Selected Homeland Security Presidential Directive 12 (HSPD-12) Requirements for Personal Identity Verification of Federal Employees and Contractors (Audit Report No. A-000-08-00X-P).

The following are our management decision and corrective actions regarding the proposed audit recommendation:

Recommendation No. 1*: We recommend that USAID's Chief Information Officer develop and document an implementation plan for Personal Identity Verification Part II, and submit the plan to the Office of Management and Budget. In developing this plan, consideration should be given to explore other options to implement Homeland Security Presidential Directive-12.*

The Offices of the CIO and Security agree with the recommendation. We have prepared a draft joint CIO and SEC HSPD-12 implementation plan and have summarized it below. We plan to finalize this plan by June 2008. The successful implementation of HSPD-12 is dependent upon consistent and adequate funding, resource availability and top management support. The HSPD Implementation plan will be flexible in order to respond to changing requirements, standards, guidelines and technology. The CIO will ensure that the HSPD-12 requirements are met and will report our progress periodically to the OIG. We plan to implement HSPD-12 requirements in four phases:

Phase I (CIO)

Phase I is Personal Identity Verification (PIV) I and II compliance with background checks, enrollment (sponsorship, two forms of identification, digital photograph, biometrics) and issuance of a compliant Federal ID card. The Agency is almost 100% compliant with the objectives for background checks, enrollment and card issuance for new employees. The target completion date for enrollment and card issuance for all current employees and contractors working in USAID/Washington is June 2009.

Target completion date: June 2009 for USAID/Washington; June 2012 for overseas employees (dependent on DoS implementation)

Phase II (SEC)

Phase II consists of physical security upgrades necessary to enable physical access to USAID/Washington using the new PIV card. The first part will consist of an upgrade to software of the current access control system and replacement card readers in order to use the PIV card for basic physical access. The second part is to design and engineer a replacement of the current aging access control system. We will initiate planning for this project when: 1) the Agency has made a final decision on whether to use the DoS IDMS, purchase an independent IDMS which replicates data to DoS, or seek another alternative; 2) when funding becomes available for planning/design, engineering, procurement and implementation of this project and 3) the appropriate MOUs and/or agreements are reached with DoS.

Target completion date: December 2010 - USAID/W; Overseas (not applicable)

Phase III (may run concurrently with Phase IV) (CIO)

Phase III will include desktop upgrades to use new PIV card with readers, biometric data and encryption hardware to enable employees to use the new credential for authentication and authorization (includes Public Key Infrastructure).

Target completion date: December 2013 - USAID/W; and December 2017 USAID Overseas

Phase IV (CIO)

Phase IV will address the feasibility of integrating the IDMS with related independent systems (e.g., access control system for physical access, systems used for logical access, HR system, personnel security databases, etc.). The goal of this phase is to ensure that the IDMS (or other designated system) is the system of authority for data.

Target completion date-: December 2013 USAID/W and December 2017 USAID Overseas

Since the field work was completed, USAID has issued 1036 credentials. We now have two operational enrollment and issuance stations which has doubled our capacity to issue credentials. For FY08, the HSPD-12 program is slated for $1.80 million in capital investment funds. We requested $2.0 million in funding for the HSPD-12 program for FY2009. We have initiated a weekly USAID HSPD-12 Implementation group to monitor progress and ensure coordination with Agency stakeholders. We have partnered with DoS (with OMB concurrence) and believe the partnership has already paid dividends by allowing USAID to:

- Accelerate implementation timeframes;
- Reduce implementation costs for HSPD-12 requirements;
- Realize efficiencies in eliminating redundant infrastructure and;
- Enhance Interoperability – Much easier to ensure interoperability across a limited number of systems.

If you have questions or need additional information, please contract Shirl Hendley, M/CIO at 202-712-4704 or Lorrie Meehan, (SEC), 202-712-5338.

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