



NOTE: The Acquisition portion of the guidance has been moved to ADS 302.



USAID
FROM THE AMERICAN PEOPLE

Acquisition & Assistance Policy Directive (AAPD)

From the Director, Office of Acquisition & Assistance Issued: October 17, 2006

AAPD 06-12

Homeland Security Presidential Directive-12 (HSPD-12) Implementation

Subject Category: **Acquisition Management; Personal Services Contracts (PSCs); Assistance Policy**

Type:

AAPDs provide information of significance to all agency personnel and partners involved in the Acquisition and Assistance process. Information includes (but is not limited to): advance notification of changes in acquisition or assistance regulations; reminders; procedures; and general information. Also, AAPDs may be used to implement new requirements on short-notice, pending formal amendment of acquisition or assistance regulations.

AAPDs are EFFECTIVE AS OF THE ISSUED DATE unless otherwise noted in the guidance below; the directives remain in effect until this office issues a notice of cancellation.

This AAPD: Is New Replaces/ Amends

Applicable to:

Existing awards; Modification required

No later than

As noted in guidance below

RFPs/RFAs and resulting awards

Other or N/A

Precedes change to:

AIDAR and Appendices D and J

USAID Automated Directives System (ADS) Chapter 302 and 303

Code of Federal Regulations

Other

No change to regulations

Michael F. Walsh

PURPOSE: The purpose of this AAPD is to accomplish the following:

- 1) provide information concerning implementation of Homeland Security Presidential Directive-12 (“HSPD-12”) and its requirement for personal identity verification (PIV), and
- 2) require contracting/agreement officers to include applicable HSPD-12 clauses in those RFP/RFAs, contracts (including PSCs), grants, and cooperative agreements that require contractors or recipients to have routine physical access to USAID-controlled facilities or logical access (i.e. NMS, AIDNet, Phoenix, LOCS, etc.) to USAID’s information systems.

The effective date of this AAPD is the date of issuance.

BACKGROUND: Increasingly, contractors (including PSCs) are required to have physical access to federally controlled facilities and information systems in the performance of government contracts. On August 27, 2004, in response to the general threat of unauthorized access to Federal government physical facilities and its information systems, the President issued Homeland Security Presidential Directive (HSPD) 12. (<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>) The primary objectives of HSPD-12 are to establish a process to enhance security, increase government efficiency, reduce identity fraud, and support the fight against global terrorism by establishing a mandatory, government-wide standard for verifying identity and providing badging credentials to its employees and contractors that routinely work in federally-controlled facilities and/or have physical access to federal information systems.

In accordance with HSPD-12, this government-wide identification standard was issued in February, 2005 by the Secretary of Commerce’s National Institute of Standards and Technology (NIST), and is referred to as FIPS 201, “Personal Identity Verification” (PIV) of Federal Employees and Contractors. Federal government agencies are required to use the FIPS 201 PIV standard for identifying and issuing new “smart card” ID to all individuals that routinely work in federally controlled facilities, or require access to federal information systems. The new ID will contain a computer chip of agency specific information. When HSPD-12 and FIPS 201 are fully implemented, there will be interoperability among federal agencies with respect to these new “smart card” ID, allowing them to be accepted by fellow agencies as reliable identification.

Although HSPD-12 and FIPS 201 only mention employees and contractors, USAID is aware that there may be situations that require assistance recipients (e.g. Fellows) to work in USAID controlled space and/or use USAID information systems. As a result, USAID has decided, as a matter of policy, to also apply the requirements of HSPD-12 to those applicable assistance awards. This AAPD addresses the impact of HSPD-12 on contractors/recipients that routinely access USAID space and/or require logical access to our information systems (i.e. access to NMS, AIDNet, Phoenix, LOCS, etc). [Guidance on the treatment of direct hire employees is outside the scope of this AAPD and is being addressed through other Agency avenues.]

IMPLEMENTATION ACTIONS TO DATE: In response to HSPD-12, on October 18, 2005, USAID issued a General Notice containing its initial HSPD-12 policy guidance (see USAID General Notice 10/18/2005, Homeland Security Presidential Directive (HSPD-12 found at <http://iapp1.usaid.gov/notices/notDetail.cfm?msgID=10497&currmo=10&curryr=2005&prevnext=yes>) HSPD-12 and its FIPS 201 PIV standard, are being implemented throughout the government in phases. USAID and other Federal Agencies, began the first phase of personal identification verification (referred to as PIV I) on October 27, 2005, which primarily involved “processes”, namely the development, adoption, and accreditation of the PIV processes. Implementation of phase II (referred to

as PIV II) will begin on October 27, 2006, when USAID initiates the issuance of the new “smart card” IDs to **new** contractor/recipient employees that routinely work in USAID space and/or need logical access to USAID’s information systems. Existing contractors/recipients who currently have IDs and are already working in USAID space and/or using USAID’s information systems, will not begin receiving the new “smart card” IDs until next year, on October 27, 2007. (Exceptions would include those situations where an existing contractor/recipient loses or damages his/her existing ID and would need a replacement ID prior to Oct 27, 2007. In those situations, the existing contractor/recipient would need to follow the PIV processes described below, and be issued one of the new smart cards.)

Earlier this year, rules were issued which amended the Federal Acquisition Regulation (FAR) to reflect HSPD-12. (See FAR Case 2005-15 at <http://acquisition.gov/far/ProposedRules/05-015.pdf>; and FAR Case 2005-17 at <http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/06-7088.pdf>)

These rules amended the FAR as follows:

- Added definitions of “federal information system” and “federally-controlled facilities” at FAR 2.101;
- Added Subpart 4.13, Personal Identity Verification of Contractor Personnel, to implement FIPS 201 and associated Office of Management and Budget (OMB) guidance. This section also requires all agencies to include language implementing the HSPD Standard in applicable solicitations and contracts that require contractors to have access to a Federally-controlled facility or access to a Federal information system; (USAID’s HSPD-12 language/clause appears later in this AAPD);
- Modified the security considerations in FAR 7.105(b)(17) to require the acquisition plan to address the agency’s PIV requirements for contractors when applicable;
- Added FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel, http://www.acqnet.gov/far/current/html/52_200_206.html#wp1139617 to require the contractor to comply with the PIV process for all affected employees in accordance with agency procedures identified in the contract. This new FAR clause 52.204-9, must be included in any solicitation or contract that requires contractors to have routine access to federally controlled space and/or access to federal information systems.

GUIDANCE: Attachments I and II to this AAPD contain USAID’s acquisition and assistance HSPD-12 clause language for inclusion in applicable RFA/RFPs, contracts/assistance awards. The HSPD-12 clauses address the PIV requirements of HSPD-12. They alert contractors and recipients about the two pieces of personal identification documents they will be required to submit before they will be able to obtain a USAID ID or be granted access to USAID’s information systems. The identity source documents must come from the list of acceptable documents. The contractor/recipient must contact USAID’s Office of Security or, if award performance is overseas, the Regional Security Officer, to obtain the approved list of documents.

The acquisition HSPD-12 clause will be included in the clause section of AIDAR Part 752 and Appendices D and J. In addition, the assistance HSPD-12 clause will be added to ADS Chapter 303’s “Required as Applicable” standard provisions.

REQUIRED ACTION:

- A) With regard to RFP solicitations and contracts that require the contractor (or contractor employees to have routine physical access to USAID-controlled facilities (i.e. will be needing a ID for regular entry to USAID space), or have logical access (i.e. access to NMS, AIDNet, Phoenix, LOCS, etc) to USAID’s information systems, Contracting Officers must include both FAR clause 52.204-9 and the USAID acquisition clause that appears in Attachment 1. Timing for inclusion of these two clauses is as follows:

- **New RFPs and new contracts (including PSCs and task orders) issued or awarded after effective date of this AAPD:** FAR 52.204-9 and USAID's attached HSPD-12 clause (attachment 1) must be included at time of solicitation and in the resultant award;
- **Existing contracts (including PSCs and task orders) awarded on or after October 27, 2005, and RFPs that have not yet closed:** FAR 52.204-9 and USAID's HSPD clause (attachment 1) must be included as soon as possible, but no later than January 27, 2007. However, existing contracts **must** be modified earlier, if there is a need for any contract employee to receive one of the new PIV smart card IDs prior to that date.
- **Existing contracts awarded prior to October 27, 2005:** FAR 52.204-9 and USAID's HSPD-12 clause (attachment 1) must be included no later than October 27, 2007. However, existing contracts **must** be modified earlier, if there is a need for any contract employee to receive one of the new PIV smart card IDs prior to that date.

B) With regard to RFA solicitations and assistance awards that require the recipient (or recipient employees) to have routine physical access to USAID-controlled facilities (i.e. will be needing a ID for regular entry to USAID space), or have logical access (i.e. access to NMS, AIDNet, Phoenix, LOCS, etc) to USAID's information systems, Assistance Officers must include the USAID acquisition clause that appears in Attachment 2. Timing for inclusion of this one clause is as follows:

- **New RFAs and new assistance awards issued or awarded after effective date of this AAPD:** USAID's HSPD-12 clause (attachment 2) must be included at time of RFA solicitation and in the resultant award;
- **Existing assistance instruments awarded on or after October 27, 2005, and RFAs that have not yet closed:** USAID's HSPD-12 clause (attachment 2) must be included as soon as possible, but no later than January 27, 2007. However, existing assistance awards **must** be modified earlier, if there is a need for any recipient employee to receive one of the new PIV smart card IDs prior to that date.
- **Existing assistance instruments awarded prior to October 27, 2005:** USAID's HSPD-12 clause (attachment 2) must be included no later than October 27, 2007. However, existing assistance awards **must** be modified earlier, if there is a need for any recipient employee to receive one of the new PIV smart card IDs prior to that date.

Point of Contact: Rosella Marshall, M/OAA/P, (202) 712-0643.

Attachment 1 - Acquisition

Homeland Security Presidential Directive-12 (HSPD-12) (September 2006)

In response to the general threat of unauthorized access to federal facilities and information systems, the President issued Homeland Security Presidential Directive-12. HSPD-12 requires all Federal agencies to use a common Personal Identity Verification (PIV) standard when identifying and issuing access rights to users of Federally-controlled facilities and/or Federal Information Systems. USAID will begin issuing HSPD-12 “smart card” IDs to applicable contracts, using a phased approach. Effective October 27, 2006, USAID will begin issuing new “smart card” IDs to new contractors (and new contractor employees) requiring routine access to USAID controlled facilities and/or access to USAID’s information systems. USAID will begin issuance of the new smart card IDs to existing contractors (and existing contractor employees) on October 27, 2007. (Exceptions would include those situations where an existing contractor (or contractor employee) loses or damages his/her existing ID and would need a replacement ID prior to Oct 27, 2007. In those situations, the existing contractor (or contractor employee) would need to follow the PIV processes described below, and be issued one of the new smart cards.)

Accordingly, before a contractor (including a PSC* or a contractor employee) may obtain a USAID ID (new or replacement) authorizing him/her routine access to USAID facilities, or logical access to USAID’s information systems, the individual must provide two forms of identity source documents in original form and a passport size photo. One identity source document must be a valid Federal or state government-issued picture ID. (Overseas foreign nationals must comply with the requirements of the Regional Security Office.) USAID/W contractors must contact the USAID Security Office to obtain the list of acceptable forms of documentation, and contractors working in overseas Missions must obtain the acceptable documentation list from the Regional Security Officer. Submission of these documents, and related background checks, are mandatory in order for the contractor to receive a building access ID, and before access will be granted to any of USAID’s information systems. All contractors must physically present these two source documents for identity proofing at their USAID/W or Mission Security Briefing. The contractor or his/her Facilities Security Officer must return any issued building access ID and remote authentication token to USAID custody upon termination of the individual’s employment with the contractor or completion of the contract, whichever occurs first.

The contractor must comply with all applicable HSPD-12 and PIV procedures, as described above, and any subsequent USAID or government-wide HSPD-12 and PIV procedures/policies, including any subsequent related USAID General Notices, Office of Security Directives and/or Automated Directives System (ADS) policy directives and required procedures. This includes HSPD-12 procedures established in USAID/Washington and those procedures established by the overseas Regional Security Office.

In the event of inconsistencies between this clause and later issued Agency or government-wide HSPD-12 guidance, the most recent issued guidance should take precedence, unless otherwise instructed by the Contracting Officer.

The contractor is required to include this clause in any subcontracts that require the subcontractor or subcontractor employee to have routine physical access to USAID space or logical access to USAID’s information systems.

Attachment 2 - Assistance

Homeland Security Presidential Directive-12 (HSPD-12) (September 2006)

In response to the general threat of unauthorized access to federal facilities and information systems, the President issued Homeland Security Presidential Directive-12. HSPD-12 requires all Federal agencies to use a common Personal Identity Verification (PIV) standard when identifying and issuing access rights to users of Federally-controlled facilities and/or Federal Information Systems. USAID is applying the requirements of HSPD-12 to applicable assistance awards. USAID will begin issuing HSPD-12 “smart card” IDs to applicable recipients (and recipient employees), using a phased approach. Effective October 27, 2006, USAID will begin issuing new “smart card” IDs to new recipients (and recipient employees) requiring routine access to USAID controlled facilities and/or access to USAID’s information systems. USAID will begin issuance of the new smart card IDs to existing recipients (and existing recipient employees) on October 27, 2007. (Exceptions would include those situations where an existing recipient (or recipient employee) loses or damages his/her existing ID and would need a replacement ID prior to Oct 27, 2007. In those situations, the existing recipient (or recipient employee) would need to follow the PIV processes described below, and be issued one of the new smart cards.)

Accordingly, before a recipient (including a recipient employee) may obtain a USAID ID (new or replacement) authorizing him/her routine access to USAID facilities, or logical access to USAID’s information systems, the individual must provide two forms of identity source documents in original form and a passport size photo. One identity source document must be a valid Federal or state government-issued picture ID. (Overseas foreign nationals must comply with the requirements of the Regional Security Office.) USAID/W recipients (and recipient employee) must contact the USAID Security Office to obtain the list of acceptable forms of documentation, and recipients working in overseas Missions must obtain the acceptable documentation list from the Regional Security Officer. Submission of these documents, and related background checks, are mandatory in order for the recipient (or employee) to receive a building access ID, and before access will be granted to any of USAID’s information systems. All recipients (or employees) must physically present these two source documents for identity proofing at their USAID/W or Mission Security Briefing. The recipient (or employee) must return any issued building access ID and remote authentication token to USAID custody upon termination of the individual’s employment with the recipient or completion of the award, whichever occurs first.

The recipient must comply with all applicable HSPD-12 and PIV procedures, as described above, as well as any subsequent USAID or government-wide HSPD-12 and PIV procedures/policies, including any subsequent applicable USAID General Notices, Office of Security Directives and/or Automated Directives System (ADS) policy directives and required procedures. This includes HSPD-12 procedures established in USAID/Washington and those procedures established by the overseas Regional Security Office. In the event of inconsistencies between this clause and later issued Agency or government-wide HSPD-12 guidance, the most recent issued guidance should take precedence, unless otherwise instructed by the Agreement Officer.

The recipient is required to include this clause in any subawards (including subcontracts) that require the subawardee or subawardee employee to have routine physical access to USAID space or logical access to USAID’s information systems.