GSA

FEB 3 2006

GSA Office of the Chief Acquisition Officer

GSA Acquisition Letter V-06-02

MEMORANDUM FOR ALL GSA CONTRACTING ACTIVITIES

FROM: EMILY W. MURPHY
CHIEF ACQUISITION OFFICER

SUBJECT: Applicability of Homeland Security Presidential Directive (HSPD) 12 to GSA Contracting Activities

1. Purpose. The purpose of this Acquisition Letter is to expand on GSA Acquisition Alert 2005-07, Applicability of Homeland Security Presidential Directive (HSPD) 12 to GSA Contracting Activities

2. Background. On December 2, 2005, GSA OCAO issued Acquisition Alert Number 2005-07, Applicability of Homeland Security Presidential Directive (HSPD) 12 to GSA contracting activities. The Alert gave some initial guidance on how GSA should implement HSPD-12. The Alert also stated that OCAO would provide additional guidance upon the issuance of the new FAR rule. The new FAR rule was issued in the January 3, 2006 edition of the Federal Register (Reference Item Number II, FAR Case 2005-015, Common Identification Standard for Contractors).

3. Effective Date. February 3, 2006.

4. Termination Date. This Acquisition Letter will expire one year from issuance unless cancelled or extended.

5. Applicability. This Acquisition Letter applies to all GSA contracting activities and to all contracts GSA issues, including those issued on behalf of other agencies. Each contracting activity in each region should take appropriate steps to communicate the policy set forth in paragraph 7 to agencies they award contracts and place orders on behalf of.

6. Reference to regulations. Federal Acquisition Regulation (FAR) Parts 2, 4, 7, and 52 are revised as a result of implementing HSPD-12. General Services Administration Acquisition Manual (GSAM) Parts 502, 504, 507, and 552 revisions are pending. See Chief People Officer Memorandum for Heads of Services and Staff Offices Regional Administrators, Subject: Background Investigation Changes Required by HSPD-12, dated October 26, 2005.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

7. Instructions/procedures.

HSPD-12 requires agencies to adopt a Governmentwide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. The FAR has been revised to require solicitations and contracts that include requirements for contractors to have access to federally controlled facilities and information systems to comply with the agency's personal identity verification process.

This Acquisition Letter is being issued to inform all GSA contracting activities that they must include the FAR clause as well as any agency-specific guidance for personal identity verification in all solicitations and contracts issued and awarded on or after October 27, 2005. FAR case 2005-015, Common Identification Standard for Contractors, that adds the required FAR language to implement HSPD-12 has been issued as an interim rule, meaning although the rule is not yet final, it is effective now (Rule became effective on January 3, 2006, see copy attached to this Acquisition Letter). Contracting activities must amend solicitations and modify contracts they have issued and awarded on or after October 27, 2005, to include the new FAR language. Contracts awarded prior to October 27, 2005, that are still active (more than 3 months away from expiration), must be modified by October 27, 2007, to include the new FAR language as well as agency-specific changes that are in accordance with agency implementation of Federal Information Processing Standards Publication (FIPS Pub) 201 and Office of Management and Budget (OMB) guidance M-05-24 (copy attached). For your information, FIPS Pub 201 can be found at: http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf.

In order to achieve the requirements of HSPD-12, the Smart Card initiative has been transferred to the Office of the Chief Information Officer. A dedicated Program Management Office (PMO) has been established and the Chief Information Officer has appointed Jack L. Finley as Program Manager of the GSA Smart Card/HSPD-12 PMO. The PMO has developed Standard Operating Procedures (SOP) for GSA HSPD-12 personal identity verification. The SOP is included as an attachment to this acquisition letter. At Appendix A in the SOP are the "Costs for Security Clearances and Public Trust Certifications." Contracting activities should advise program/requiring officials of these costs.

Attachments:
OMB Memorandum M-05-24, Implementation of HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors

FAR Interim Rule, Common Identification Standard for Contractors

GSA HSPD-12 Personal Identity Verification – I (PIV-I) Standard Operating Procedure

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

M-05-24

August 5, 2005

MEMORANDUM FOR THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

SUBJECT: Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors

On August 27, 2004, the President signed HSPD-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" (the Directive). The Directive requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. As required by the Directive, the Department of Commerce issued Federal Information Processing Standard 201 (the Standard). This memorandum provides implementing instructions for the Directive and the Standard.

Inconsistent agency approaches to facility security and computer security are inefficient and costly, and increase risks to the Federal government. Successful implementation of the Directive and the Standard will increase the security of your Federal facilities and information systems. As noted in the attached guidance, this standard identification applies to your employees and contractors who work at your facilities or have access to your information systems. Following implementation, Federal departments and agencies will be able to recognize and accept this common identification standard.

It is important to note the use of standard identification does not replace your existing law or OMB policy responsibilities; including the laws and policies governing personnel security, acquisition, and information technology security law.

If you have questions about this guidance, contact Jeanette Thornton, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget. Phone (202) 395-3562, fax (202) 395-5167, or e-mail: eauth@omb.eop.gov.

Attachments

A) HSPD-12 Implementation Guidance for Federal Departments and Agencies
B) HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors

Attachment A

HSPD-12 IMPLEMENTATION GUIDANCE FOR FEDERAL DEPARTMENTS AND AGENCIES

1. **To whom does the Directive apply?**
2. **What is the schedule for implementing the Directive?**
3. **How should I implement Part 1 of the Standard?**
4. **How should I implement Part 2 of the Standard?**
5. **What acquisition services are available?**
6. **How must I consider privacy in implementing the Directive?**
7. **Is there anything else I must consider or know?**

1. To whom does the Directive apply?

As defined below, Department and Agency heads must conduct a background investigation, adjudicate the results, and issue identity credentials to their employees and contractors who require long-term access to Federally controlled facilities and/or information systems.

A. Departments and Agencies

- "Executive departments" and agencies listed in title 5 U.S.C. § 101, and the Department of Homeland Security; "independent establishments" as defined by title 5 U.S.C. §104(1); and the United States Postal Service (title 39 U.S.C § 201).

Does **not** apply to:

- "Government corporations" as defined by title 5 U.S.C. § 103(1) are encouraged, but not required to implement this Directive.

B. Employee

- Federal employees, as defined in title 5 U.S.C § 2105 "Employee," within a department or agency.
- Individuals employed by, detailed to or assigned to a department or an agency.
- Within the Department of Defense (DoD) and the Department of State (DoS), members of the Armed Forces, Foreign Service, and DoD and DoS civilian employees (including both appropriated fund and non-appropriated fund employees).
- Applicability to other agency specific categories of individuals (e.g., short-term (i.e. less than 6 months) guest researchers; volunteers; or intermittent, temporary or seasonal employees) is an agency risk-based decision.

Does **not** apply to:

- Within DoD and DoS, family members and other eligible beneficiaries.
- Occasional visitors to Federal facilities to whom you would issue temporary identification.

C. Contractor

- Individual under contract to a department or agency, requiring routine access to federally controlled facilities and/or federally controlled information systems to whom you would issue Federal agency identity credentials, consistent with your existing security policies.

Does **not** apply to:

- Individuals under contract to a department or agency, requiring only intermittent access to federally controlled facilities.

D. Federally Controlled Facilities

- Federally-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of a department or agency covered by this Directive.
- Federally controlled commercial space shared with non-government tenants. For example, if a department or agency leased the 10th floor of a commercial building, the Directive applies to the 10th floor only.
- Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.
- Facilities under a management and operating contract. Such as for the operation, maintenance, or support of a Government-owned or-controlled research, development, special production, or testing establishment.

E. Federally Controlled Information Systems

- Information technology system (or information system), as defined by the Federal Information Security Management Act of 2002 (44 U.S.C. § 3502(8)).
- Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency (44 U.S.C. § 3544(a)(1)(A)).
- Applicability for access to Federal systems from a non-Federally controlled facility (e.g. a researcher up-loading data through a secure website or a contractor accessing a government system from their own facility) should be based on the risk determination required by existing National Institute of Standards and Technology (NIST) guidance.[1]

Does **not** apply to:

- Identification associated with national security systems as defined by the Federal Information Security Management Act of 2002 (44 U.S.C. § 3542(2)(A)).[2]

---

[1] Federal Information Processing Standard (FIPS 199): Standards for Security Categorization for Federal Information and Information Systems, 2/04, http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[2] See NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System, 8/03, http://www.csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf.

2. **What is the schedule for implementing the Directive?**

A. **The Department of Commerce's National Institute of Standards and Technology (NIST) shall meet the following milestones:**

Date	Department of Commerce Action
2/25/05	HSPD-12 Standard Published –Federal Information Processing Standard 201 (FIPS 201)[3]
6/25/05	Technical reference implementation released
8/5/05	Conformance testing information released

B. **All covered departments and agencies shall complete the following actions:**

Date	Agency Action
6/27/05	Implementation plans submitted to OMB
8/26/05	Provide list of other potential uses of Standard (see question 7)
10/27/05	Comply with FIPS 201, Part 1 (see question 3)
10/27/06	Begin compliance with FIPS 201, Part 2 (see question 4)
10/27/07	Verify and/or complete background investigations for all current employees and contractors (see question 3)
10/27/08	Complete background investigations for all Federal department or agency employees employed over 15 years (see question 3)

C. **The General Services Administration (GSA) shall complete the following actions:**

Date	General Services Administration Action
7/31/05	Establish authentication acquisition services (see question 5)
10/27/05	Sponsor Federal Acquisition Regulation (FAR) amendment implementing the Standard.

3. **How should I implement Part 1 of the Standard?**

The Standard, required by HSPD-12, contains two parts to guide department and agency implementation. The requirements of part 2 build upon the requirements of part 1. They are:

- **Part 1: Common Identification, Security and Privacy Requirements** – minimum requirements for a Federal personal identification system that meets the control and security objectives of the Directive, including the personal identity proofing, registration, and issuance process for employees and contractors.

[3] FIPS 201: Personal Identity Verification for Federal Employees and Contractors, 2/25/05, http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf. All technical documents are available at http://www.csrc.nist.gov/piv-project/.

- **Part 2: Government-wide Uniformity and Interoperability** – Detailed specifications to support technical interoperability among departments and agencies, including card elements, system interfaces, and security controls required to securely store and retrieve data from the card.

For all new employees, contractors and other applicable individuals your department or agency must by October 27, 2005:

A. **Adopt and accredit a registration process** consistent with the identity proofing, registration and accreditation requirements in section 2.2 of the Standard and forthcoming technical guidance issued by NIST, regardless of whether your agency will be ready to issue standard compliant identity credentials by October 27, 2005. This registration process will apply to all new identity credentials issued (i.e. no new identity credentials can be issued until these conditions are met).[4]

B. **Initiate the National Agency Check with Written Inquiries (NACI) or other suitability or national security investigation prior to credential issuance**. Before issuing the credential, agencies should receive notification of results of the National Agency Checks.[5] If you do not receive the results in 5 days, the identity credential can be issued based on the FBI National Criminal History Check (fingerprint check).[6]

Identity credentials issued to individuals without a completed NACI or equivalent must be electronically distinguishable (i.e. information is stored in the data on the card) from identity credentials issued to individuals who have a completed investigation. The Department of Commerce will provide the electronic format for this information.

Agencies shall not re-adjudicate individuals transferring from another department or agency provided: 1) possession of a valid Federal identity credential can be verified by the individual's former department or agency, and 2) the individual has undergone the required NACI or other suitability or national security investigation at individual's former agency.

Since Foreign National employees and contractors may not have lived in the United States long enough for a NACI to be meaningful, agencies should conduct an equivalent investigation, consistent with your existing policy. OMB will establish an interagency working group to explore whether guidance is necessary with respect to background investigations for foreign national employees and contractors.

---

[4] NIST Special Publication 800-79: Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, 7/05, http://www.csrc.nist.gov/piv-project/publications/sp800-79.pdf.

[5] The National Agency Checks are the Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), FBI Name Check, and FBI National Criminal History Fingerprint Check. The National Agency Check with Written Inquiries includes all of the National Agency Checks plus searches of records covering specific areas of an individual's background during the past five years.

[6] Section 2.2 of the Standard has been revised to clarify for the initial credential issuance, only the fingerprint check must be completed.

C. **Include language implementing the Standard in applicable new contracts.** All new contracts (including exercised options) requiring contractors (as defined in 1.C. above) to have long term access to federally controlled facilities or access to federally controlled information systems shall include a requirement to comply with the Directive and Standard for affected contractor personnel. Agencies must comply with the forthcoming Federal Acquisition Regulation sections on these requirements.

For current employees, contractors and other applicable individuals, your department or agency must by October 27, 2005:

D. **For current employees,** develop a plan and begin the required background investigations for all current employees who do not have an initiated or successfully adjudicated investigation (i.e., "completed National Agency Check with Written Inquires or other Office of Personnel Management [OPM] or National Security community investigation") on record. By October 27, 2007 verify and/or complete background investigations for all current employees.

At card renewal (every 5 years), the NACI requirements should be followed in accordance with OPM guidance. Currently OPM does not have a requirement to reinvestigate employees, not otherwise subject to an investigation (e.g. for a security clearance).

For individuals who have been Federal department or agency employees over 15 years, a new investigation may be delayed, commensurate with risk, but must be completed no later than October 27, 2008.

E. **For current contractors and other applicable individuals,** develop a plan and begin the required background investigations for all current contractors who do not have a successfully adjudicated investigation on record. Phase in this requirement to coincide with the contract renewal cycle, but no later than October 27, 2007.

4. How should I implement Part 2 of the Standard?

By October 27, 2006, all departments and agencies must begin deploying products and operational systems meeting these requirements:

A. **Issue and require the use of identity credentials for all new employees and contractors,** compliant with Parts 1 and Part 2 of the Standard. For current employees and contractors, phase in issuance and use of identity credentials meeting the Standard to end no later than October 27, 2007.

B. **Implement the technical requirements of the Standard** in the areas of personal authentication, access controls and card management, consistent with the Standard (i.e. sections 3, 4, and 5) and NIST Special Publication 800-73.[7]

C. **Risk Based Facility Access** – Use the appropriate card authentication mechanism described in section 6 of the Standard, with minimal reliance on visual authentication to the maximum extent practicable (section 6.2.1). Officials who control access shall determine the appropriate mechanism based on risk determinations.

D. **Use of Digital Certificates** – Compliance with the Standard requires the activation of at least one digital certificate on the identity credential for access control. This digital certificate (and any optional digital certificates on the identity credential) must originate from:

1) An agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher by December 31, 2005; or

2) An approved Shared Service Provider.[8]

Agencies must require the use of the identity credential for system access. Prioritize this requirement based on risk, using your authentication risk assessments required by previous OMB guidance and the categorization required by FIPS 199.[9] Document the results and make available to your Chief Information Officer, security office and Inspector General's Office upon request.

You are already required to have rules of behavior in place (including the consequences for violation) before employees and contractors are granted access to systems.[10] All employees and contractors must have access to this documentation.

5. What acquisition services are available?

A. **Requirement to use federally approved products and services** – To ensure government-wide interoperability, all departments and agencies must acquire products and services that are approved to be compliant with the Standard and included on the approved products list. A forthcoming Federal Acquisition Regulation will require the use of only approved products and services.

---

[7] NIST Special Publication 800-73: Integrated Circuit Card for Personal Identity Verification, 4/8/05, http://www.csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf.

[8] OMB Memorandum M-05-05: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services, 12/20/04, http://www.whitehouse.gov/omb/memoranda/fy2005/m05-05.pdf.

[9] OMB Memorandum M-04-04: E-Authentication Guidance for Federal Agencies, 12/16/03, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf and FIPS 199: Standards for Security Categorization for Federal Information and Information Systems, 2/04, http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[10] See OMB Circular A-130 at http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.

B. **Use of GSA Acquisition Services** – GSA has been designated as the "executive agent for Government-wide acquisitions of information technology" under section 5112(e) of the Clinger-Cohen Act of 1996 (40 U.S.C. § 11302(e)) for the products and services required by the Directive. GSA will report to OMB annually on the activities undertaken as an executive agent.

GSA will make approved products and services available through blanket purchase agreements (BPA) under Federal Supply Schedule 70 for Information Technology, a schedule under the Multiple Award Schedules (MAS) Program. When developing BPAs, GSA will ensure all approved suppliers provide products and services that meet all applicable federal standards and requirements.

Departments and agencies are encouraged to use the acquisition services provided by GSA. Any agency making procurements outside of GSA vehicles for approved products must certify the products and services procured meet all applicable federal standards and requirements, ensure interoperability and conformance to applicable federal standards for the lifecycle of the components, and maintain a written plan for ensuring ongoing conformance to applicable federal standards for the lifecycle of the components.

C. **Sponsorship** – For small departments and agencies and agencies who share facilities with another agency it may not be cost effective to procure your own products or services. GSA will identify agency sponsors who will provide a range of services to agencies. The extent and cost of services to be provided will be determined by agreement between the sponsor and the customer agency.

6. How must I consider privacy in implementing the Directive?

You are already required under the Privacy Act of 1974 (5 U.S.C. § 552a), the E-Government Act of 2002 (44 U.S.C. ch. 36), existing OMB policy and section 2.4 of the Standard to satisfy privacy and security requirements. Implementing the Directive does not alter these requirements. In addition, **prior to identification issuance you must:**

A. Ensure personal information collected for employee and contractor identification purposes is handled consistent with the Privacy Act of 1974 (5 U.S.C. § 552a).

B. Assign an individual to be responsible for overseeing the privacy-related matters associated with implementing this Directive.

C. Submit to OMB, and make publicly available, a comprehensive privacy impact assessment (PIA) of your HSPD-12 program, including analysis of the information technology systems used to implement the Directive. The PIA must comply with section 208 of the E-Government Act of 2002 (44 U.S.C. ch. 36) and OMB Memorandum M-03-22 of September 26, 2003, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002." You must periodically review and update the privacy impact assessment. Email your completed PIA to pia@omb.eop.gov.

D. Update the pertinent employee and contractor identification systems of records notices (SORNs) to reflect any changes in the disclosure of information to other Federal agencies (i.e. routine uses), consistent with Privacy Act of 1974 (5 U.S.C. § 552a) and OMB Circular A-130, Appendix 1.[11] These SORNs should be periodically re-reviewed to ensure accuracy.

E. Collect information using only forms approved by OMB under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. ch. 35), where applicable. Departments and agencies are encouraged to use Standard Form 85, Office of Personnel Management Questionnaire for Non-Sensitive Positions (OMB No. 3206-0005) or the Standard Form 85P, Office of Personnel Management Questionnaire for Positions of Public Trust (OMB No. 3206-0005) when collecting information. If you plan to collect information from individuals covered by the PRA using a new form you must obtain OMB approval of the collection under the PRA process.

F. Develop, implement and post in multiple locations (e.g., agency intranet site, human resource offices, regional offices, provide at contractor orientation, etc.) your department's or agency's identification privacy act statement/notice, complaint procedures, appeals procedures for those denied identification or whose identification credentials are revoked, and sanctions for employees violating agency privacy policies.

G. Adhere to control objectives in section 2.1 of the Standard. Your department or agency may have a wide variety of uses of the credential not intended or anticipated by the Directive. These uses must be appropriately described and justified in your SORN(s) and PIA.

Note: OMB has established a small working group to develop model language for common portions of the SORN, PIAs and Privacy Act Statements for department and agency use when implementing the Directive. These products will be completed no later than October 27, 2005.

7. Is there anything else I must consider or know?

A. **Paragraph 5 of the Directive** asks departments or agencies to "identify those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are **important for security** and for which use of the Standard in circumstances not covered by this Directive should be considered" by August 26, 2005. This determination should be consistent with the privacy requirements specified in question 6 of this guidance and should include any uses of the Standard not meeting the control objectives listed in the Standard. If you have identified other facilities, information systems or applications, submit them to the Assistant to the President for Homeland Security, with an electronic copy to the Office of Management and Budget at eauth@omb.eop.gov.

[11] See http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.

B. **Annual Reporting** – The applicability section of the Standard requires annual reporting on the numbers of agency issued credentials, to include the respective numbers of agency-issued 1) general credentials and 2) special-risk credentials (issued under the Special-Risk Security Provision on page v of the Standard). Future OMB guidance will address this requirement.

C. **Biometrics Implementation** – This OMB guidance is being issued before finalization of NIST Special Publication 800-76: Biometric Data Specifications for Personal Identity Verification. Agencies may defer the capture of biometrics for the identity credential until the NIST guidance is final.

D. **Employees Serving Undercover** – Agencies with employees who serve undercover shall implement this Directive in a manner consistent with maintenance of the cover, and to the extent consistent with applicable law and policy.

E. **Relationship to Personnel Security Clearances** –The directive reaffirms the existing requirement, first enumerated in Executive Order 10450 of April 27, 1953 to conduct background investigations on all Federal employees. This investigation is used to determine suitability. Thus, the investigation required by the directive is not the same as the investigations required for personnel security clearances or for public trust determinations. The issuance of a security clearance is a discrete privilege and should be done in accordance with applicable standards. Personnel security investigations for the purpose of issuing security clearances or for the purpose of making public trust determinations can be sufficient for the required background investigations required by the directive.

F. **Applying guidance to temporary employees and contractors** – The requirements for temporary employees and contractors should be viewed as the minimum requirements, dependent on risk and other factors. Agencies who employ temporary personnel (e.g. contract employment under special arrangements with schools, businesses, state and local governments, etc.) should apply this guidance as follows:

- **Employed greater than 6 months** – Apply all sections of this guidance, including the background investigation requirements in the Standard (e.g. "completed National Agency Check with Written Inquires [NACI] or other Office of Personnel Management or National Security community investigation").

- **Employed 6 months or less**
  a) Apply adequate controls to systems and facilities (i.e. ensuring temporary staff has limited/controlled access to facilities and information systems).
  b) Provide temporary employees and contractors with clear documentation on the rules of behavior and consequences for violation before granting access to facilities and/or systems.
  c) Document any security violations involving these employees, and report them to the appropriate authority within 24 hours.

d) Identity credentials issued to these individuals must be visually and electronically distinguishable from identity credentials issued to individuals to whom the Standard does apply. Agencies should be careful not to develop policies which overlap or contradict the Standard's processes for identity proofing and issuance.

- **Occasional visitors**
  a) Apply adequate controls to systems and facilities (i.e. ensuring visitors have limited/controlled access to facilities and information systems).
  b) Develop agency-specific visitor policies (as appropriate).

Attachment B

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-12

August 27, 2004

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b) (2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

# # #

GSA HSPD-12 Personal Identity Verification - I (PIV-I)
Standard Operating Procedure (SOP)
October 27, 2005
Version 1.0

INTRODUCTION:

Homeland Security Presidential Directive – 12 (HSPD-12) is a directive establishing a common identification standard for federal employees and contractors. The four control objectives associated with HSPD-12 are:

1) Identification is issued based on sound criteria for verifying an individual employee's identity

2) Identification is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation

3) Identification can be rapidly authenticated electronically

4) Identification is issued only by providers whose reliability have been established by an official accreditation process

Federal Information Processing Standard – 201 (FIPS-201), created by the National Institute for Standards and Technology (NIST), describes the federal policy for compliance with HSPD-12. FIPS 201 is comprised of two major components, Personal Identity Verification I and II (PIV- I and PIV-II). PIV- I defines the standards required for complying with identity proofing and registration of applicants and issuance and maintenance of a PIV card. PIV- II defines the standards required for complying with the technology and interoperability components of HSPD-12. Federal Agencies are required to comply with the control objectives for PIV- I no later than October 27, 2005, and begin complying with the control objectives for PIV- II no later than October 27, 2006. The purpose of this document is to convey GSA's HSPD-12 procedure for compliance with the requirements of PIV- I.

GSA must conduct a background investigation, adjudicate the results and issue identity credentials to its associates and contractors who require long-term access to its federally controlled facilities and/or information systems.

For more detailed information on the HSPD-12 PIV- I requirements, please refer to the Federal Identity Management Handbook, which can be located at the following website: http://cio.gov/ficc/documents/FedIdentityMgmtHandbook.pdf.

This SOP modifies procedures for obtaining GSA nationwide credentials for all GSA federal associates and contractors issued after October 27, 2005. The procedures will supplement instructions contained in ADM P7640.2, GSA Nationwide Credentials Handbook, until the Handbook is revised. In the event that this SOP contradicts the GSA Nationwide Credentials Handbook, this SOP takes precedence.

The GSA regional offices may choose to issue temporary credentials to associates or contractors that require immediate access to GSA facilities and/or information systems prior to the adjudication of the National Criminal History Fingerprint Check and the initiation of the NACI.

1.0 REQUIREMENTS FOR GSA PIV- I IDENTITY PROOFING AND REGISTRATION:

1.1 Starting October 27, 2005 GSA must use an approved identity proofing and registration process that complies with FIPS 201 for all employees and contractors requesting a GSA ID.

1.2. Identity proofing requires the initiation of a National Agency Check with Written Inquiries (NACI) or an equivalent Office of Personnel Management (OPM) or National Security investigation. For new hires, HR Services will initiate the background checks. For current associates, this requirement is satisfied if the employee has a completed and successfully adjudicated NACI on file. For contractors, the managing office is responsible for requesting the background checks.

1.3. During registration, the applicant must provide two identity source documents in original form. The documents must be on the list of acceptable documents included in *I-9, OMB No. 1115-0136, Employment Eligibility*. One of the documents must be a valid (not expired) picture ID issued by a state government or the Federal Government.

1.4. The new PIV identity-proofing and registration process must adhere to the principle of separation of roles. No single individual may have the ability to request issuance of a new PIV credential without the approval of a second authorized person.

1.5. The ID Card applicant must appear at least once in person in front of an authorized PIV official.

2.0 REQUIREMENTS FOR GSA PIV- I ISSUANCE AND MAINTENANCE:

2.1. GSA must use an approved, certified and documented ID Card issuance and maintenance process.

2.2. The ID Card issuance process must include the initiation of a NACI or other OPM or National Security community investigation required for Federal employment and the completion and successful adjudication of an FBI Criminal History Fingerprint Check.

2.3. The GSA ID Card must be revoked or withheld if the results of these checks are deemed to be non-satisfactory by GSA.

2.4. Prior to issuing a GSA ID Card to an applicant, associate or contractor, the authorized GSA issuer must complete the chain of trust by validating the applicant's picture on the credential with the valid (not expired) picture ID issued by a state government or the Federal Government.

2.5. The FBI National Criminal History Fingerprint Check must be completed and adjudicated and the NACI initiated before the ID Card can be issued.

2.6. GSA must issue credentials through systems and providers whose reliability has been established by GSA and documented and approved in writing.

3.0 GSA PIV-I HIGH LEVEL OVERVIEW OF ROLES AND RESPONSIBILITES:

Section 4 Steps	Role	Responsibility	Description	PIV Requirement	Training Plan	Who at GSA?
1,10	**HR Services**	Background Check	Initiate NACI/ NAC; Adjudicates background checks; Delivers NACI/NAC results information to sponsors and HSPD-12 PMO.	NAC must be completed prior to credential issuance; NACI must be initiated prior to credential issuance.	HR Services must complete training on applicable GSA procedures/policies for HSPD-12	HR for associates and contractors; DHS/FPS for contractors; PBS for Tenant contractors; NCR/ALD for small agencies.
2,7	**Applicant**	Authorized Application	Complete GSA credential application; Submit to GSA Credentialing Official; Present two forms of ID to Registrar.	Applicant presents two valid forms of ID to Registrar.	None	All new associates and contractors.
3	**Sponsor**	Approval	PIV Sponsor signs the form.	Sponsor must be authorized in writing by Agency; Sponsor must complete PIV sponsor training.	Sponsors must complete the Sponsor Training Modules prior to 10/27/05.	Current GSA "two letter officials" or designee will be the new Requesting Officials.
4,6,8,11	**Registrar (Credentialing Official)**	GSA ID Card Registration	Validate application form/replacement requests; Verify applicant's identity using two forms of ID (at least one photo ID); Verify authority of Sponsor; Capture data for PIV Card - biometrics and photographs; Submit data for PIV card production. Receives the adjudicated results from the HSPD-12 PMO confirming that the NACI has been initiated and the National Criminal History Fingerprint Check is adjudicated prior to sending the ID cards to the Issuers.	Registrar must be authorized in writing by Agency; Registrar must complete applicable PIV Registrar training.	Registrars must complete PIV Registrar training on applicable procedures/policies for HSPD-12.	Current approved GSA Credentialing Officials.
5	**Service Provider**	GSA ID Card Production	Automated process to produce PIV Card. Secure delivery of completed ID's to Credentialing Offices. No changes.	Service Provider's reliability must be established.	None	Central ID Service Provider.

8,11	GSA HSPD-12 PMO	Approval for Card Issuance	Coordinate with Credentialing Official on who can be issued credentials.	Fingerprint check must be completed prior to credential issuance; NACI must be initiated prior to credential issuance.	Complete GSA PIV training on applicable procedures/policies for HSPD-12.	HSPD-12 PMO
9	Issuer	Card Issuance	Verify recipient's identity (valid govt. picture ID) prior to credential issuance to Applicant.	Credential Issuers must be authorized in writing by GSA; Issuer must complete applicable PIV issuer training.	Authorized PIV Issuers must complete PIV Training on applicable procedures/policies for HSPD-12.	Current GSA Credentialing Issuers.

4.0 GSA PIV- I PROCEDURES:

4.1. HUMAN RESOURCES SERVICES:

- HR Services will perform the background checks (NACI/NAC/etc.) for associates and contractors as specified in the SOP for HSPD-12 Personnel Security Procedures.
- Adjudication results of the NAC are provided to the applicant's Sponsor and the HSPD-12 PMO so that ID Cards can be issued.

4.2. APPLICANT:

- An applicant requests a GSA ID. The applicant may be a new employee/contractor or an existing employee/contractor updating their information, replacing a lost ID card, or renewing an expired or non-functioning card.
- The applicant completes a GSA ID application and provides it to the GSA Sponsor.

4.3. PIV SPONSOR: (GSA Approving Official/Supervisor)

- The PIV Sponsor is the individual that is authorized to approve a GSA ID Card for the applicant. The Sponsor evaluates the applicant-provided information on the application and signs the application in the appropriate location. The PIV Sponsor may also need to indicate access rights, and special privileges necessary for the applicant.
- For contractors, the managing office is responsible for ensuring the credentialing process is initiated. For contractors not supported by PBS, this includes the submission of request for the Background Check process.
- The PIV Sponsor provides the completed and signed application to the PIV Registrar (GSA Credentialing Official), in a secure manner in person by hand/interoffice mail/FedEx via a sealed and secure envelope.
- If appropriate, the PIV Sponsor is responsible for inserting the Pegasys Document Number (PDN) Number in Block J of the SF85 otherwise the process could be delayed.

Refer to Appendix A for "Costs for Security Clearances and Public Trust Certifications"

4.4. PIV REGISTRAR: (GSA Credentialing Official)

- The PIV Registrar confirms the validity of the PIV request.
- The PIV Registrar validates and verifies the correct data has been provided, is completed properly, and has been signed by authorized GSA Officials.
- The PIV Registrar can arrange an appointment with the applicant based upon the registration office schedule. During registration, the applicant must provide two identity source documents in original form. The documents must be on the list of acceptable documents included in *I-9, OMB No.1115-0136, Employment Eligibility*. One of the documents must be a valid (not expired) picture ID issued by a state government or the Federal Government.
- The PIV Registrar must meet the applicant in person and verify the applicant's identity source documents. The PIV Registrar verifies the applicant's identification by evaluating the documents. Identity source documents should be inspected visually and may be verified electronically as being unaltered and authentic. If electronic means are unavailable, the PIV Registrar will use other means to verify the identity source documents. For each identity source document, the PIV Registar must record the following information:

  - The title of the document
  - The document issuing authority
  - The document number, as listed on the document
  - The document's expiration date, if available
  - Any other information used to confirm the identity of the applicant

- The PIV Registrar must ensure that personal information collected for employees and contractor identification purposes is handled consistent with the Privacy Act of 1974 (5 U.S.C. 552a)
- The PIV Registrar signs the record of recorded information. Photocopies of the original documents ARE NOT REQUIRED.
- After verifying the applicant's identification, the PIV Registrar records the applicant's biometric data and digital photograph.
- The PIV Registrar is responsible for verifying the adjudicated results from the HSPD-12 PMO confirming that the NACI has been initiated and the National Criminal History Fingerprint Check is adjudicated, prior to sending the credentials to the PIV Issuers.

4.5. SERVICE PROVIDER:

- Completed ID Card records ready for processing are submitted electronically for card personalization. A secure process is used to transfer the information for ID Card production. Data needed by the card producer includes digital photograph, name, affiliation, contact information, biometric data, and other data associated with the applicant. Badge colors and types are determined. Badge colors and types will vary based on factors such as contractor vs. GSA associate, first responder status, and property and access rights.

- GSA ID Cards are personalized in a centralized ID Card production facility. When completed, they are delivered to the PIV Registrar via a secure method.

4.6. PIV REGISTRAR (GSA Credentialing Official):

- Upon receipt of the ID Cards from the production facility, the ID Cards should be inventoried and logged.

4.7. APPLICANT

- The Applicant completes the necessary background check forms with the HR Representative. Forms completed may include the 176T FPS Form (Statement of Personal History), the SF85 (Questionnaire for non-sensitive positions) or the SF85P (Questionnaire for Public Trust Positions). The forms are then provided to Human Resources Services for processing.

  For all new Applicants and all new Contractors, a National Agency Check with Written Inquiries (NACI) must be initiated or other national security investigation initiated and the National Criminal History Fingerprint Check adjudicated prior to PIV card issuance.

  CURRENT CARDHOLDERS – All existing employees and contractors with a completed and adjudicated NACI on record do not require additional background checks. For all existing GSA employees and contractors with no NACI on record (or other suitable investigation), a NACI must be completed and adjudicated by October 27, 2007.

  AT RENEWAL - Individuals renewing cards (every 5 years) should follow NACI requirements with OPM Guidance. Reinvestigation is not required per OMB Guidance M-05-24 dated 8/25/05.

4.8. HSPD-12 PMO / PIV REGISTRAR (GSA Credentialing Official):

- The HSPD-12 PMO informs the PIV Registrar of the results of the National Criminal History Fingerprint Check and the initiation of the NACI.

4.9. PIV ISSUER (in some cases performed by GSA Credentialing Office):

- The GSA ID Card PIV Issuer is the individual or individuals authorized to issue ID

Cards.

- The PIV Issuer notifies the applicant that the ID cards can be picked up.
- Applicant must appear in person to receive the ID card from the PIV Issuer.
- Prior to issuing a GSA ID Card to an applicant, employee or contractor, the GSA PIV Issuer must complete the chain of trust by validating the applicant's picture on the credential with a valid (not expired) picture ID issued by a state government or the Federal Government presented by the applicant.
- If this is a replacement card, the superceded card must be accounted for and/or collected prior to providing the new card.
- The PIV Issuer will distribute the card to the applicant. The PIV Issuer will obtain a signature from the applicant (current PIV cardholder) attesting to the applicant's acceptance of the PIV card and related responsibilities.

4.10. HUMAN RESOURCES SERVICES:

- The NACI adjudication results are then emailed to the PIV Sponsor and the HSPD-12 PMO via an e-mail notification.

4.11. HSPD-12 PMO/PIV REGISTRAR (GSA Credentialing Official):

- The HSPD-12 PMO informs the Credentialing official of NACI adjudication results. If the results of the NACI are favorable, then the applicant will retain the credentials with the full background investigation completed. If the results of the NACI are unfavorable, then the HSPD-12 PMO will coordinate with the Credentialing Official to possibly revoke the credentials depending on the outcome of the appeal process.

Appendix A

Costs for Security Clearances and Public Trust Certifications - Effective 10/01/2005

	Sensitivity/Risk Level	Investigation		Reinvestigation
		Priority	Standard	
NATIONAL SECURITY	Special Sensitive (Level 4) *Top Secret, SCI, and Q access*	**SSBI** -- $3,655	$3,150	PPR -- $1,900
	Critical Sensitive (Level 3) *Top Secret or Secret; also TS eligible and Q access*	**SSBI** -- $3,655	$3,150	PPR -- $1,900
	Noncritical Sensitive (Level 2) *High Risk (Level 6) w/Secret or Confidential*	**BI** -- $3,240	$2,735	PRI -- $550
	Noncritical Sensitive (Level 2) *Moderate Risk (Level 5) w/Secret or Confidential*	**LBI** -- $2,645 or **MBI** -- $550	**LBI** -- $2,265 or **MBI** -- $475	NACLC-- $205
	Noncritical Sensitive (Level 2) *Low Risk (Level 1) w/Secret or Confidential*	**ANACI** -- $226	$147	NACLC-- $205
PUBLIC TRUST	High Risk (Level 6) No access	**BI** -- $3,240	$2,735	PRI -- $550
	Moderate Risk (Level 5) No access	**LBI** -- $2,645 or **MBI** -- $550	**LBI** -- $2,265 or **MBI** -- $475	None
	Contractor Employee Moderate Risk (Level 5) No access	**SAC** (US citizen) -- $50 **SAC** (non-US) -- $56	**NACIC** -- $107	None
	Non-sensitive or Low Risk (Level 1) No access	Not available	**NACI** -- $97	None

GSA Personnel Security Requirements Division (CPR)
Phone: (202) 208-4296
E-mail: gsa.security.office@gsa.gov
Lotus Notes: GSA Security Office

Appendix B

Definitions of Terms:

Access (Logical) - An individual's ability to access one or more computer system resources such as a workstation, network, application, or database. Different access privileges are provided to different persons depending on their roles and responsibilities in the agency.

Access (Physical) - An individual's ability to access a physical location such as a building, parking lot, office, or other designated physical space. Different access privileges are assigned to different persons depending on their roles and responsibilities in the agency.

Authenticate - The process of establishing confidence of authenticity; in this case, in the validity of a person's identity and the PIV Card.

Applicant Access Rights - The process of determining what types of activities or access are permitted for a given physical or logical resource is performed by the Registrar. Once the identity of the user has been authenticated, the registrar has the authorization to determine whether the applicant has access to a specific location, system, or service.

Background Investigation – An investigation covering specific areas of a person's background. The Background Investigation consists of a record search, credit search, and a NAC, NACI, or similar OPM investigations. The investigating agency interviews the candidate and selected sources.

Biometric - A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Card Personalization - Refers to the modification of a card such that it contains data specific to the cardholder. Methods of personalization may include encoding the magnetic stripe or bar code, loading data on the ICC, or printing photo or signature data on the card.

Federal Identity Management Handbook – The Federal Identity Management Handbook was developed in collaboration with the FICC, IAB, FPKIPA, and OMB. It is offered as an implementation guide for government agency credentialing managers, their leadership, and other stakeholders as they pursue compliance with HSPD-12 and FIPS 201. The handbook provides specific implementation direction on course of action, schedule requirements, acquisition planning, migration planning, lessons learned, and case studies.

Federal Information Processing Standard (FIPS) - A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.

Federal Information Processing Standard – 201 (FIPS-201) In response to the HSPD-12 directive, the National Institute of Standards and Technology (NIST) published Federal Information Processing Standards Publication 201 (FIPS 201) on February 25, 2005. FIPS 201 and its associated Special Publications provide a detailed specification for Federal agencies and departments deploying a personal identity verification (PIV) card for their employees and contractors. The FIPS 201 standard can be accessed from the NIST web site at http://csrc.nist.gov/piv-project/index.html.

Homeland Security Presidential Directive-12 (HSPD-12) – HSPD-12 directed the creation of a common Federal standard for secure and reliable identification issued by Federal agencies for their employees and contractors.

Identity Proofing - The process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV Registrar when attempting to establish an identity.

Identity Verification - The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.

I-9, OMB No. 1115-0136, Employment Eligibility form – This is a form presented by the Applicant to the PIV Registrar to assist the Registrar in the Identity Proofing process.

National Agency check (NAC) – Record searches with selected sources covering specific areas of a person's background.

National Agency Check with Written Inquiries (NACI) – An investigation consisting of a NAC and written inquiries covering specific areas of a person's background during the past 5 years.

National Security Clearance – Certification issued by the GSA Security Officer or designee that a person may access classified information on a need-to-know basis.

National Security Position – A sensitive position under EO 10450. Usually, persons in national security positions hold security clearances, though some employees may be considered eligible for clearances rather than actively holding the clearances.

National Institute for Standards and Technology (NIST) –Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST developed the FIPS-201 document as a follow up to the HSPD-12 directive and to provide suggestions for agency implementation.

Non-sensitive position – A position that does not require access to classified information and that has low risk to the national security and public trust.

Personal Identity Verification (PIV) - A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Personal Identity Verification I (PIV I) – FIPS-201 is broken down into two major processes: PIV I and PIV II. PIV I describes the standards required for complying with identity proofing, registration, issuance and maintenance of a PIV card. The SOP focuses on the PIV I requirements.

Personal Identity Verification II (PIV II) – FIPS-201 is broken down into two major processes: PIV I and PIV II. PIV II describes the standards required for complying with the technology and interoperability components of HSPD-2.

PIV credential issuance/issuance process – When "PIV credential/badge/ID issuance or issuance process" is mentioned in this SOP it is referring to the ID badge distribution from the Issuer to the Applicant.

Successful/favorable adjudication of background check – If the Human Resources Security Office determines a favorable adjudication of the applicant's background check this indicates that the applicant is suitable for GSA hiring, and is capable of retaining a GSA credential.

Unfavorable adjudication of background check – If the Human Resources Security Office determines an unfavorable adjudication of the applicant's background check this indicates that the applicant is not suitable for GSA hiring, and the GSA credential may be revoked. If an appeal is made by the applicant this determination can be changed.

Office of Personnel Management (OPM) – The Office of Personnel Management's main role in the credentialing process is to receive background check requests from the HR Security office, perform background checks on applicants, and deliver the results of the background checks to the HR Security Office where the results will be adjudicated.

■ d. Removing the word "commercial" from paragraphs (h)(1) and (h)(2) of the clause.
■ The revised and added text reads as follows:

52.247–52 Clearance and Documentation Requirements—Shipments to DoD Air or Water Terminal Transshipment Points.

* * * * *

CLEARANCE AND DOCUMENTATION REQUIREMENTS—SHIPMENTS TO DOD AIR OR WATER TERMINAL TRANSSHIPMENT POINTS (FEB 2006)

* * * * *

(a) * * *

(3) * * *

(iv) Explosives, ammunition, poisons or other dangerous articles classified as class 1, division 1.1, 1.2, 1.3, 1.4; class 2, division 2.3; and class 6, division 6.1; or

(v) Radioactive material, as defined in 49 CFR 173.403, class 7.

* * * * *

52.247–64 [Amended]

■ 49. Amend section 52.247–64 by—
■ a. Revising the date of the clause to read "(FEB 2006)";
■ b. Removing from paragraph (e)(1) of the clause "of the Panama Canal Commission or";
■ c. Revising the date of Alternate II to read "(FEB 2006)"; and
■ d. Removing from paragraph (e)(1) of Alternate II "of the Panama Canal Commission or".
■ 50. Revise section 52.247–67 to read as follows:

52.247–67 Submission of Transportation Documents for Audit.

As prescribed in 47.103–2, insert the following clause:

SUBMISSION OF TRANSPORTATION DOCUMENTS FOR AUDIT (FEB 2006)

(a) The Contractor shall submit to the address identified below, for prepayment audit, transportation documents on which the United States will assume freight charges that were paid—

(1) By the Contractor under a cost-reimbursement contract; and

(2) By a first-tier subcontractor under a cost-reimbursement subcontract thereunder.

(b) Cost-reimbursement Contractors shall only submit for audit those bills of lading with freight shipment charges exceeding $100. Bills under $100 shall be retained on-site by the Contractor and made available for on-site audits. This exception only applies to freight shipment bills and is not intended to apply to bills and invoices for any other transportation services.

(c) Contractors shall submit the above referenced transportation documents to—

_____

_____

_____

[*To be filled in by Contracting Officer*]

(End of clause)

■ 51. Section 52.247–68 is added to read as follows:

52.247–68 Report of Shipment (REPSHIP).

As prescribed in 47.208–2, insert the following clause:

REPORT OF SHIPMENT (REPSHIP) (FEB 2006)

(a) *Definition. Domestic destination,* as used in this clause, means—

(1) A destination within the contiguous United States; or

(2) If shipment originates in Alaska or Hawaii, a destination in Alaska or Hawaii, respectively.

(b) Unless otherwise directed by the Contracting Officer, the Contractor shall—

(1) Send a prepaid notice of shipment to the consignee transportation officer—

(i) For all shipments of—

(A) Classified material, protected sensitive, and protected controlled material;

(B) Explosives and poisons, class 1, division 1.1, 1.2 and 1.3; class 2, division 2.3 and class 6, division 6.1;

(C) Radioactive materials requiring the use of a III bar label; or

(ii) When a truckload/carload shipment of supplies weighing 20,000 pounds or more, or a shipment of less weight that occupies the full visible capacity of a railway car or motor vehicle, is given to any carrier (common, contract, or private) for transportation to a domestic destination (other than a port for export);

(2) Transmits the notice by rapid means to be received by the consignee transportation officer at least 24 hours before the arrival of the shipment; and

(3) Send, to the receiving transportation officer, the bill of lading or letter or other document containing the following information and prominently identified as a "Report of Shipment" or "REPSHIP FOR T.O."

REPSHIP FOR T.O. 81 JUN 01
TRANSPORTATION OFFICER
DEFENSE DEPOT, MEMPHIS, TN.
SHIPPED YOUR DEPOT 1981 JUN 1 540 CTNS MENS COTTON TROUSERS, 30,240 LB, 1782 CUBE, VIA XX-YY*
IN CAR NO. XX 123456**-BL***-C98000031****CONTRACT DLA_____ETA*****-JUNE 5 JONES & CO., JERSEY CITY, N.J.

*Name of rail carrier, trucker, or other carrier.

**Vehicle identification.

***Bill of lading.

****If not shipped by BL, identify lading document and state whether paid by contractor.

*****Estimated time of arrival.

(End of clause)

PART 53—FORMS

■ 52. Revise section 53.247 to read as follows:

53.247 Transportation (U.S. Commercial Bill of Lading).

The commercial bill of lading is the preferred document for the transportation of property, as specified in 47.101.

[FR Doc. 05–24546 Filed 12–30–05; 8:45 am]
BILLING CODE 6820–EP–S

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 2, 4, 7, and 52

[FAC 2005–07; FAR Case 2005–015; Item II]

RIN 9000–AK35

Federal Acquisition Regulation; Common Identification Standard for Contractors

AGENCIES: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Interim rule with request for comments.

SUMMARY: The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) have agreed on an interim rule amending the Federal Acquisition Regulation (FAR) to address the contractor personal identification requirements in Homeland Security Presidential Directive (HSPD–12), "Policy for a Common Identification Standard for Federal Employees and Contractors," and Federal Information Processing Standards Publication (FIPS PUB) Number 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors."

DATES: *Effective Date:* January 3, 2006.

Comment Date: Interested parties should submit written comments to the FAR Secretariat on or before March 6, 2006 to be considered in the formulation of a final rule.

Applicability Date: This rule applies to solicitations and contracts issued or awarded on or after October 27, 2005. Contracts awarded before that date requiring contractors to have access to a Federally controlled facility or a Federal

information system must be modified by October 27, 2007, pursuant to FAR subpart 4.13 in accordance with agency implementation of FIPS PUB 201 and OMB guidance M–05–24.

ADDRESSES: Submit comments identified by FAC 2005–07, FAR case 2005–015, by any of the following methods:

- Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.
- Agency Web Site: *http://www.acqnet.gov/far/ProposedRules/proposed.htm*. Click on the FAR case number to submit comments.
- E-mail: *farcase.2005–015@gsa.gov*. Include FAC 2005–07, FAR case 2005–015 in the subject line of the message.
- Fax: 202–501–4067.
- Mail: General Services Administration, Regulatory Secretariat (VIR), 1800 F Street, NW, Room 4035, ATTN: Laurieann Duarte, Washington, DC 20405.

Instructions: Please submit comments only and cite FAC 2005–07, FAR case 2005–015, in all correspondence related to this case. All comments received will be posted without change to *http://www.acqnet.gov/far/ProposedRules/proposed.htm*, including any personal and/or business confidential information provided.

FOR FURTHER INFORMATION CONTACT: For clarification of content, contact Mr. Michael Jackson, Procurement Analyst, at (202) 208–4949. Please cite FAC 2005–07, FAR case 2005–015. For information pertaining to status or publication schedules, contact the FAR Secretariat at (202) 501–4755.

SUPPLEMENTARY INFORMATION:

A. Background

Increasingly, contractors 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 physical facilities and information systems, the President issued Homeland Security Presidential Directive (HSPD–12). The primary objectives of HSPD–12 are to establish a process to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Governmentwide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. In accordance with HSPD–12, the Secretary of Commerce issued on February 25, 2005, Federal Information Processing Standards Publication (FIPS PUB) 201, Personal Identity Verification of Federal Employees and Contractors, to establish a Governmentwide standard for secure and reliable forms of identification for Federal and contractor employees. FIPS PUB 201 is available at *http://www.csrc.nist.gov/publications/fips/fips201/FIPS–201–022505.pdf*. The associated Office of Management and Budget (OMB) guidance, M–05–24, dated August 5, 2005, can be found at *http://www.whitehouse.gov/omb/memoranda/fy2005/m05–24.pdf*.

In accordance with requirements in HSPD–12, by October 27, 2005, agencies must—

(a) Adopt and accredit a registration process consistent with the identity proofing, registration and accreditation requirements in section 2.2 of FIPS PUB 201 and associated guidance issued by the National Institute for Standards and Technology. This registration process applies to all new identity credentials issued to contractors;

(b) Begin the required identity proofing requirements for all current contractors that do not have a successfully adjudicated investigation (*i.e.*, completed National Agency Check with Written Inquires (NACI) or other Office of Personnel Management or National Security community investigation) on record. (By October 27, 2007, identity proofing should be verified and completed for all current contractors);

(c) Complete and receive notification of results of the FBI National Criminal History Check prior to credential issuance;

(d) Include language implementing the Standard in applicable solicitations and contracts that require contractors to have access to a federally-controlled facility or access to a Federal information system; and

(e) Complete the applicable privacy requirements listed in section 2.4 of FIPS PUB 201 and the OMB guidance M–05–24.

The rule amends the FAR by—

- Adding the definitions "Federal information system" and "Federally-controlled facilities" at FAR 2.101;
- Adding Subpart 4.13, Personal Identity Verification of Contractor Personnel, to implement FIPS PUB 201 and the associated OMB guidance;
- Modifying the security considerations in FAR 7.105(b)(17) to require the acquisition plan to address the agency's personal identity verification requirements for contractors when applicable;
- Adding FAR clause 52.204–9, Personal Identity Verification of Contractor Personnel, to require the contractor to comply with the personal identity verification process for all affected employees in accordance with agency procedures identified in the contract.

This is not a significant regulatory action and, therefore, was not subject to review under Section 6(b) of Executive Order 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

B. Regulatory Flexibility Act

The changes may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601 *et seq.*, because all entities that hold contracts or wish to hold contracts that require their personnel to have access to Federally controlled facilities or information systems will be required to employ on Government contracts only employees who meet the standards for being credentialed and expend resources necessary to help employees fill out the forms for credentialing. An Initial Regulatory Flexibility Analysis (IRFA) has been prepared. The analysis is summarized as follows:

INITIAL REGULATORY FLEXIBILITY ANALYSIS

FAR Case 2005–015

Common Identification Standard for Contractors

This Initial Regulatory Flexibility Analysis (IRFA) has been prepared consistent with 5 U.S.C. 603.

1. Description of the reasons why the action is being taken.

This proposed rule implements Homeland Security Presidential Directive (HSPD–12), "Policy for a Common Identification Standard for Federal Employees and Contractors." This directive requires agencies to adopt a Governmentwide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. As required by the Directive, the Department of Commerce issued Federal Information Processing Standard Publication (FIPS PUB) 201. Consequently, the FAR must be revised to require solicitations and contracts include requirements that contractors who have access to federally-controlled facilities and information systems comply with the agency's personal identify verification process. Failure to take action would expose the Government to unacceptable risk of harm to employees and assets.

2. Succinct statement of the objectives of, and legal basis for, the rule.

This rule is being promulgated to ensure that Federal agencies consistently apply the requirements of HSPD–12 to Federal contracts. Consistency in an identification standard is cost effective and will improve the security of Government employees and assets.

FIPS PUB 201 states that the Personal Identity Verification (PIV) Registrar shall initiate a National Agency Check with Inquiries (NACI) on the applicant as required by Executive Order 10450. Any unfavorable results of the investigation shall be adjudicated to determine the suitability of the applicant for obtaining a PIV credential. When all of the requirements have been completed, the PIV Registrar notifies the sponsor and the designated PIV issuer that the applicant has been approved for the issuance of a PIV credential. Conversely, if any of the required steps are unsuccessful, the PIV Registrar shall send appropriate notifications to the same authorities.

3. Description of and, where feasible, estimate of the number of small entities to which the rule will apply.

This rule will apply to any contractor whose employees will have access to Federal facilities or information systems. A precise estimate of the number of small entities that fall within the rule is not currently feasible because it would include both contractors who perform in Government-owned space as well as those who perform in Government-leased space (including employees of the lessor and its contractors.)

4. Description of projected reporting, recordkeeping, and other compliance requirements of the rule, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for preparation of the report or record.

The rule does not directly require reporting, recordkeeping or other compliance requirements within the meaning of the Paperwork Reduction Act (PRA). The rule does require that any entity, including small businesses that will be performing a contract that requires its employees to have access to Federal facilities or information systems, submit information on their employees. Such information will include a personnel history for each employee having access to a Federal facility or information system for a period exceeding 6 months. Although the forms involved are similar to a standard application for employment that is used by many companies, it is envisioned that some employers, especially those using non-skilled or semi-skilled laborers, will need to help their employees complete the form. It is estimated that each applicant will spend approximately 30 minutes completing the form.

5. Identification, to the extent practicable, of all relevant Federal rules which may duplicate, overlap, or conflict with the rule.

The Councils are unaware of any duplicative, overlapping or conflicting Federal rule. To the extent that there may be a duplicative, overlapping or conflicting Federal rule, the purpose of this rule is to establish a Federal standard that would eliminate such duplication, overlap or conflict.

6. Description of any significant alternatives to the rule which accomplish the stated objectives of applicable statutes and which minimize any significant economic impact of the rule on small entities.

There are no practical alternatives that will accomplish the objectives of HSPD–12.

The FAR Secretariat has submitted a copy of the IRFA to the Chief Counsel for Advocacy of the Small Business Administration. Interested parties may obtain a copy from the FAR Secretariat. The Councils will consider comments from small entities concerning the affected FAR Parts 2, 4, 7, and 52 in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C 601, *et seq.* (FAC 2005–07, FAR case 2005–015), in correspondence.

C. Paperwork Reduction Act

The Paperwork Reduction Act does not apply because the changes to the FAR do not impose information collection requirements that require the approval of the Office of Management and Budget under 44 U.S.C. 3501, *et seq.*Further, the OMB guidance, M–05–24, advises to collect information using only forms approved by OMB under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. ch. 35), where applicable. Departments and agencies are encouraged to use Standard Form 85, Office of Personnel Management Questionnaire for Non-Sensitive Positions (OMB No. 3206–0005), or the Standard Form 85P, Office of Personnel Management Questionnaire for Positions of Public Trust (OMB No. 3206–0005), when collecting information.

D. Determination to Issue an Interim Rule

A determination has been made under the authority of the Secretary of Defense (DOD), the Administrator of General Services Administration (GSA), and the Administrator of the National Aeronautics and Space Administration (NASA) that urgent and compelling reasons exist to promulgate this interim rule without opportunity for public comment. This action is necessary to implement HSPD–12 which directs agencies to require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to federally-controlled facilities and access to federally-controlled information systems no later than October 27, 2005. The issuance of this interim rule will not be the first time the public has seen and had a chance to comment on FIPS PUB 201 and HSPD–12. The Department of Commerce, National Institute of Standards and Technology, issued a draft of FIPS PUB 201 on November 23, 2004, with comments due by December 23, 2004. Also, OMB issued a notice of Draft Agency Implementation Guidance for HSPD–12 on April 8, 2005, with comments due by May 9, 2005. HSPD–12 requires the development and agency implementation of a mandatory Governmentwide standard for secure and reliable forms of identification for both Federal employees and contractors. However, pursuant to Public Law 98–577 and FAR 1.501, the Councils will consider public comments received in response to this interim rule in the formation of the final rule.

List of Subjects in 48 CFR Parts 2, 4, 7, and 52

Government procurement.

Dated: December 22, 2005.

Gerald Zaffos,

Director, Contract Policy Division.

■ Therefore, DoD, GSA, and NASA amend 48 CFR parts 2, 4, 7, and 52 as set forth below:

■ 1. The authority citation for 48 CFR parts 2, 4, 7, and 52 continues to read as follows:

Authority: 40 U.S.C. 121(c); 10 U.S.C. chapter 137; and 42 U.S.C. 2473(c).

PART 2—DEFINITIONS OF WORDS AND TERMS

■ 2. Amend section 2.101 in paragraph (b)(2) by adding, in alphabetical order, the definitions "Federal information system" and "Federally-controlled facilities" to read as follows:

2.101 Definitions.

* * * * *

(b) * * *

(2) * * *

Federal information system means an information system (44 U.S.C. 3502(8)) used or operated by a Federal agency, or a contractor or other organization on behalf of the agency.

Federally-controlled facilities means—

(1)(i) Federally-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of a department or agency;

(ii) Federally-controlled commercial space shared with non-government tenants. For example, if a department or agency leased the 10th floor of a commercial building, the Directive applies to the 10th floor only; and

(iii) Government-owned, contractor-operated facilities, including laboratories engaged in national defense research and production activities.

(2) The term does not apply to educational institutions that conduct activities on behalf of departments or agencies or at which Federal employees are hosted unless specifically designated as such by the sponsoring department or agency.

* * * * *

PART 4—ADMINISTRATIVE MATTERS

■ 3. Add Subpart 4.13, consisting of sections 4.1300 and 4.1301, to read as follows:

Subpart 4.13—Personal Identity Verification of Contractor Personnel

Sec.
4.1300 Policy.
4.1301 Contract clause.

4.1300 Policy.

(a) Agencies must follow Federal Information Processing Standards Publication (FIPS PUB) Number 201, "Personal Identity Verification of Federal Employees and Contractors," and the associated Office of Management and Budget (OMB) implementation guidance for personal identity verification for all affected contractor and subcontractor personnel when contract performance requires contractors to have physical access to a federally-controlled facility or access to a Federal information system.

(b) Agencies must include their implementation of FIPS PUB 201 and OMB guidance M–05–24, dated August 5, 2005, in solicitations and contracts that require the contractor to have physical access to a federally-controlled facility or access to a Federal information system.

(c) Agencies shall designate an official responsible for verifying contractor employee personal identity.

4.1301 Contract clause.

The contracting officer shall insert the clause at 52.204–9, Personal Identity Verification of Contractor Personnel, in solicitations and contracts when contract performance requires contractors to have physical access to a federally-controlled facility or access to a Federal information system.

PART 7—ACQUISITION PLANNING

■ 4. Amend section 7.105 by revising paragraph (b)(17) to read as follows:

7.105 Contents of written acquisition plans.

* * * * *

(b) * * *

(17) *Security considerations.* For acquisitions dealing with classified matters, discuss how adequate security will be established, maintained, and monitored (see Subpart 4.4). For information technology acquisitions, discuss how agency information security requirements will be met. For acquisitions requiring contractor physical access to a federally-controlled facility or access to a Federal information system, discuss how agency requirements for personal identity verification of contractors will be met (see Subpart 4.13).

* * * * *

PART 52—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 5. Add section 52.204–9 to read as follows:

52.204–9 Personal Identity Verification of Contractor Personnel.

As prescribed in 4.1301, insert the following clause:

PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2006)

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive–12 (HSPD–12), Office of Management and Budget (OMB) guidance M–05–24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal information system.

(End of clause)

[FR Doc. 05–24547 Filed 12–30–05; 8:45 am]
BILLING CODE 6820–EP–S

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 2, 7, 11, 12, 16, 37, and 39

[FAC 2005–07; FAR Case 2003–018; Item III]

RIN 9000–AK00

Federal Acquisition Regulation; Change to Performance-based Acquisition

AGENCIES: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Final rule.

SUMMARY: The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) have agreed on a final rule amending the Federal Acquisition Regulation (FAR) by changing the terms "performance-based contracting (PBC)" and "performance-based service contracting (PBSC)" to "performance-based acquisition (PBA)" throughout the FAR; adding applicable PBA definitions of "Performance Work Statement (PWS)" and "Statement of Objectives (SOO)" and describing their uses; clarifying the order of precedence for requirements; eliminating redundancy where found; modifying the regulation to broaden the scope of PBA and give agencies more flexibility in applying PBA methods to contracts and orders of varying complexity; and reducing the burden of force-fitting contracts and orders into PBA, when it is not appropriate. The title of the rule has also been changed to reflect the deletion of "service."

DATES: *Effective Date:* February 2, 2006.

FOR FURTHER INFORMATION CONTACT: For clarification of content, contact Mr. Michael Jackson, Procurement Analyst, at (202) 208–4949. Please cite FAC 2005–07, FAR case 2003–018. For information pertaining to status or publication schedules, contact the FAR Secretariat at (202) 501–4755.

SUPPLEMENTARY INFORMATION:

A. Background

DoD, GSA, and NASA published a proposed rule in the **Federal Register** at 69 FR 43712 on July 21, 2004, to which 15 commenters responded. In addition, three respondents submitted comments in response to FAR Case 2004–004, Incentive for Use of Performance-Based Contracting for Services, that the Councils determined are more relevant to this FAR case. The major changes to the proposed rule that resulted from the public comments and Council deliberations are:

(1) *FAR 2.101 Definitions.* REVISED the definition of PBA to clarify its meaning.

(2) *FAR 2.101 Definitions.* REVISED the definition of PWS to clarify its meaning.

(3) *FAR 2.101 Definitions.* REVISED the definition of SOO to clarify its meaning.

(4) *FAR 7.103(r) Agency-head responsibilities.* DELETED "and, therefore, fixed-price contracts" from the statement "For services, greater use of performance-based acquisition methods and, therefore, fixed-price contracts * * * should occur for follow-on acquisitions" because the Councils