




**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

#