OFFICE OF MANAGEMENT AND BUDGET
[2005N__]
Office of E-Government and Information Technology: Notice of Draft Department and Agency Implementation Guidance for Homeland Security Presidential Directive 12

AGENCY: Office of Management and Budget, Executive Office of the President.

ACTION: Notice and request for comments.

SUMMARY: The Office of Management and Budget requests comments on the draft department and agency implementation guidance on Homeland Security Presidential Directive 12(HSPD-12). The guidance is posted at http://www.whitehouse.gov/omb/inforeg/infopoltech.html.

DATES: To ensure consideration of comments, comments must be in writing and received by OMB no later than [30 days from published in Federal Register].

ADDRESSES: Comments on this Notice should be addressed to Jeanette Thornton, Office of E-Government and Information Technology. You are encouraged to submit these comments by e-mail to eauth@omb.eop.gov. You may submit via facsimile to (202) 395-5167. Comments can be mailed to the attention of Ms. Michele Courtney, General Services Administration Office of Identity Policy and Practices Division (MEI), 1800 F Street, NW, Room 2014 Washington, DC, 20405.

FOR FURTHER INFORMATION CONTACT: Ms. Jeanette Thornton, Office of Information Technology and E-Government, Office of Management and Budget, Washington, DC 20503. Telephone: (202) 395-3562, e-mail to eauth@omb.eop.gov.

SUPPLEMENTARY INFORMATION: On August 27, 2004 the President signed HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors. The Secretary of Commerce was asked to issue, by February 27, 2005, a Government-wide standard for secure and reliable forms of identification to be issued by the Federal Government to its employees and contractors. This standard (Federal Information Processing Standard (FIPS) 201: Personal Identity Verification for Federal Employees and Contractors) was issued on February 25, 2005 and can be found at: http://www.csrc.nist.gov/piv-project/.

The Director of the Office of Management and Budget was asked to ensure agency compliance with this Directive. This agency implementation guidance provides specific instructions to agency heads on how to implement the Directive and the Department of Commerce Standard (FIPS 201). To better inform your comments, first read FIPS 201.

On January 19, 2005 the General Services Administration, in partnership with the Department of Commerce and the Office of Management and Budget, held a public meeting to address the privacy and security concerns as they may affect individuals, including Federal employees and contractors as well as the public at large, in implementation. This meeting informed this implementation guidance.

Dated:

Karen S. Evans,
Administrator for
E-Government and Information Technology.

DRAFT HSPD-12 Implementation Guidance for Federal Departments and Agencies

1. To whom does the directive apply?

As defined below, Department and Agency heads must 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 5 U.S.C. §101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. §104(1); and the United States Postal Service.
- Government corporations as defined by 5 U.S.C. §103(1) are encouraged, but not required to implement this Directive.

B. Employee and Contractor

- Federal employees, as defined in title 5 U.S.C §2105 "Employee," within a department or agency. Applicability of the directive to other agency specific categories of individuals (e.g., guest researchers) is an agency decision.
- Individuals under contract to the Federal government, to whom you would issue long-term Federal agency identity credentials, consistent with your existing security policies.
- Within the Department of Defense (DOD), the Directive applies to members of the Armed Forces and DOD civilian employees (including both appropriated fund and nonappropriated fund employees). This directive does **not** apply to retirees, family members, and non-military eligible beneficiaries.
- Directive does **not** apply to short-term guests and occasional visitors to Federal facilities to whom you would issue temporary identification.

C. 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, this Directive applies to the 10th floor only.
- Does **not** apply to academic locations who conduct activities on behalf of department or agencies or at which Federal employees may be hosted unless specifically designated by the sponsoring department or agency.

D. 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. §3544(a)(1)(A)(ii)) "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."
- Applicability for the access of Federal systems by remote access is a department or agency decision (e.g. researchers' up-loading data through a secure website).

2. What is the schedule for implementing the directive?

A. The Department of Commerce shall meet the following milestones:

Date	Department of Commerce Action
2/25/05	Publish HSPD-12 Standard–Federal Information Processing Standard 201 (FIPS 201)[1]
4/29/05	Publish related technical specifications (NIST Special Publications 800-73 and 800-76)[2]
6/25/05	Release reference implementation to aid agency implementation
8/5/05	Release conformance testing information

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

Date	Agency Action
6/27/05	Submit implementation plan (guidance provided in separate OMB Memorandum)
8/27/05	Provide list of other potential uses of Standard (see section 7)
10/27/05	Comply with FIPS 201, Part 1 (see section 3)
10/27/06	Comply with FIPS 201, Part 2 (see section 3)

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

[1]Federal Information Processing Standard 201: Personal Identity Verification for Federal Employees and Contractors, February 25, 2005. Available at: http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf.

[2] NIST Special Publication 800-73: Integrated Circuit Card for Personal Identity Verification and NIST Special Publication 800-76 Biometric Data Specification for Personal Identity Verification. Standards will be posted on March 15, 2005 at http://csrc.nist.gov/publications/nistpubs/index.html.

Date	General Services Administration Action
3/14/05	Publish Federal Identity Management Handbook[3]
7/31/05	Establish authentication acquisition services (see section 4)
10/27/05	Issue a Federal Acquisition Regulation (FAR) amendment implementing the Standard.

3. How should I implement the directive?

The Standard contains two parts to guide department and agency implementation. The requirements of part 2 build upon the requirements of part 1. The parts are:

Part 1: Common Identification, Security and Privacy Requirements – The 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.

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.

Part 1: Common Identification, Security and Privacy Requirements

By October 27, 2005 all identification issued by your department or agency must:

A. **Satisfy the control objectives in Section 2.1** of the Standard for all new identity credentials issued to employees and contractors.

B. **Adopt and accredit a registration process** consistent with the identity proofing and registration requirements in section 2.2 of the Standard. This registration process applies for all new identity credentials issued. For existing employees and contractors, develop a plan and begin completing the required identity proofing requirements for all current employee and contractors who do not have an investigation (i.e., "completed National Agency Check with Written Inquires or other Office of Personnel Management or National Security community investigation") on record. The investigation must be verifiable.

C. **Include language implementing the Standard in applicable contracts.** This language should apply to individuals under contract to the Federal government, to whom you would issue long-term Federal agency identification, consistent with your existing security policies. Additional information will be included in a FAR amendment.

D. **Complete the privacy requirements** listed in section 5 of this guidance.

[3] See Federal Identity Management Handbook Public Draft, http://www.cio.gov/ficc/documents/FedIdentityMgmtHandbook.pdf.

Departments and agencies whose identity credentials can be verified electronically must:

E. **Rapidly authenticate** – Have mechanisms in place to take advantage of this capability in a manner that enables rapid authentication of the credential. Rapid authentication is the ability to check if the identity credential is valid without undue delay.

Part 2: Government-wide Uniformity and Interoperability

By October 27, 2006 all departments and agencies must meet these requirements:

A. **Technical requirements –** Implement the interoperable identity credentials in the areas of personnel authentication, access controls and card management, consistent with the Standard and related NIST Special Publications. These requirements are specified in sections 3, 4, and 5 of the Standard.

B. **Credential issuance –** Require the use of identity credentials for all new employees and contractors that are compliant with Part 2. Phase in issuance of cards for current employees and contractors meeting the standard.

C. **Credential authentication –** Use the appropriate card authentication mechanism described in section 6 of the standard, with minimal reliance on visual authentication (section 6.2.1). Officials responsible for controlling access shall determine the appropriate mechanism.

D. **Identity verification –** Demonstrate substantial progress in completing identity proofing for current employees and contractors who do not meet the part 1 requirements. **By September 30, 2007, identity proofing should be on record for all current employees and contractors.**

E. **System access –** Compliance with the Standard requires the activation of at least one digital certificate on the identity credential for access control, the requirement to use this capability for access control to specific agency networks and systems should be based on the department's or agency's authentication risk assessments, required by OMB Memorandum M-04-04 of December 16, 2003, "E-Authentication Guidance for Federal Agencies." Ideally (but not required) employee and contractor system access should make use of the identity credential as part of the system access protocol. Systems categorized as high-impact systems under FIPS-199 Standards for Security Categorization for Federal Information and Information Systems should receive priority integrating identity credentials into system access processes. [4]

[4] OMB Memorandum M-04-04, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf. December 14, 2003, and FIPS 199 http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf , December 2003.

4. What acquisition services are available?

A. **Preapproval of Products and Services –**To ensure government-wide interoperability, products and services procured by departments or agencies will be preapproved as meeting the standard. GSA, in partnership with the Department of Commerce will establish a process to ensure all suppliers of the technology used to implement this directive are compliant with the Standard and can demonstrate the established criteria are met.

B. **GSA Services –** GSA is hereby designated as "an 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 establish several procurement services for optional agency-use including the use of Multiple Award Schedules and blanket purchase agreements. Departments and agencies should only procure preapproved products and services.

Departments and agencies are encouraged to use the acquisition services developed by the GSA. GSA will report to OMB annually on the activities undertaken as an executive agent.

By March 15, 2005, GSA, in partnership with the Federal Identity Credentialing Committee, will release an HSPD-12 implementation handbook for public comment to provide additional information.

C. **Agency Customization –** When implementing the standard, all mandatory requirements in the Standard must be met. Customization is permitted in limited circumstances, provided it does not interfere with interoperability nor diminish the security requirements specified in the Standard and is approved by OMB.

5. How must I consider privacy in implementing the directive?

When 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), and existing OMB policy to satisfy privacy and security requirements. See section 2.4 of the standard for a summary of the privacy requirements. In addition, **prior to identification issuance or by October 27, 2005 you must:**

A. Ensure that personal information collected for employee 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. Prepare and submit to OMB a comprehensive privacy impact assessment 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 pertinent employee-identification systems of records (SOR) notice(s) 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.

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

F. Develop, implement and post in appropriate locations (e.g., agency intranet site, human resource offices, regional offices, etc.) your department's or agency's identification privacy policy, complaint procedures, appeals procedures for those denied identification or whose identification credentials are revoked, 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 and its components not intended or anticipated by the Directive.

6. What is the relationship to National Security Systems and Personnel Security Clearances?

A. The directive reaffirms the existing requirement in Executive Order 10450 of April 27, 1950 to conduct a background investigation on Federal employees. The investigation is used to prove your identity and worthiness to hold a position of public trust. Thus, the investigation required by the directive is not the same as the more stringent investigation required for personnel security clearances for access to classified information.

B. This directive does **not** apply to identification associated with national security systems as defined under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. §1452).

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 27, 2005. This determination should be consistent with the privacy requirements specified in section 5 of this guidance. Submit this information electronically to Jeanette Thornton, Office of Management and Budget at eauth@omb.eop.gov.

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). This reporting will be incorporated into your agencies annual report on the Federal Information Security Management Act of 2002 (44 U.S.C. §3544(a)(1)(A)(ii)) and will be detailed in future OMB guidance.

C. **Impact of Future Technical Guidance to Issued by the Department of Commerce –** This OMB guidance is being put out for public comment when NIST Special Publication 800-73: Integrated Circuit Card for Personal Identity Verification is not finalized. The draft version of the NIST Special Publication will specify that if your agency has not implemented a large scale deployment of identity credentials, you should implement the Part 2 specification stipulated in the Standard and supporting SP 800-73. If your agency has a large scale deployment you can use the interim transitional phase described in the Special Publication.

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

Attachment

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-12

August 27, 2004

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-12

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

# # #