



DEPARTMENT OF THE TREASURY
WASHINGTON, DC 22202

**Acquisition Procedures
Update (APU)
No. 2012-03
September 11, 2012**

MEMORANDUM FOR BUREAU CHIEF PROCUREMENT OFFICERS

FROM: Thomas A. Sharpe, Jr
Senior Procurement Executive
Office of the Procurement Executive

**Thomas
Sharpe**

Digitally signed by Thomas Sharpe
DN: c=US, o=U.S. Government,
ou=Department of the Treasury,
ou=Departmental Offices, ou=People,
serialNumber=SH2056, cn=Thomas
Sharpe
Date: 2012.09.12 08:36:28 -04'00'

James A. Thomas, Jr
Program Executive Officer for
Treasury Enterprise Identity, Credential and
Access Management (TEICAM)

Digitally signed by James Thomas
DN: c=US, o=U.S. Government,
ou=Department of the Treasury,
ou=Departmental Offices,
ou=People, serialNumber=TH0692,
cn=James Thomas
Date: 2012.09.11 14:04:19 -04'00'

**SUBJECT: Office of Management and Budget (OMB) Requirements for
Continued Implementation of Homeland Security Presidential
Directive (HSPD) 12 Policy for a Common Identification
Standard for Federal Employees and Contractors**

- 1. Purpose:** To update the Department of the Treasury requirements for acquisitions conducted in support of Homeland Security Presidential Directive-12 (HSPD-12) “*Policy for a Common Identification Standard for Federal Employees and Contractors*”. This Acquisition Procedures Update (APU) incorporates current Office of Management and Budget (OMB) requirements outlined in OMB memorandum M-11-11.
- 2. Effective Date:** Immediately.
- 3. Expiration Date:** When cancelled or superseded.
- 4. Background:** HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials. On February 3, 2011, OMB issued memorandum M-11-11, “*Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*,” which directed federal agencies to expedite their use of the PIV credentials for access to federal facilities, networks and information systems. In July 2011, Treasury released TD 71-12, “*Treasury Guide for Homeland Security Presidential Directive 12*” and in September 2011, the Treasury Assistant Secretary for Management signed the revised TD 71-12, “*Homeland Security Presidential Directive 12 Policy*”. TD 71-12 establishes Treasury-wide policy for HSPD-12 implementation.

This APU sets forth Treasury-specific contracting policy for the acquisition of products and services in support of the implementation of HSPD-12.

5. DTAP Updates:

Accordingly, the following subpart is inserted in DTAP:

“Subpart 1004.13 Personal Identity Verification

1004.1302 Acquisition of Approved Products and Services for Personal Identity Verification.

(a) Procurements for services and products involving Physical Access Control Systems (PACS) or Logical Access Control Systems (LACS) must be in accordance with all applicable Federal Homeland Security Presidential Directive-12 (HSPD-12) policy and the Federal Acquisition Regulation (FAR). Additionally, in order to ensure government-wide interoperability, OMB Memorandum 06-18, “Acquisition of Products and Services for Implementation of HSPD-12” requires agencies to acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications. PACS and LACS are defined as follows:

- 1) Physical Access Control Systems (PACS) - An electronic system that controls the ability of people or vehicles to enter a protected area, by means of authentication and authorization at access control points. System components may include, but not limited to, the following: card readers, control panels, servers and software.
- 2) Logical Access Control Systems (LACS) - Systems which authenticate and authorize an individual to access federally controlled information systems. System components may include, but are not limited to, the following: laptops, desktops, servers, mobile devices and software.

(b) When procuring products and services in support of HSPD-12 to:

- 1) enable all new PACS and LACS under development to use Personal Identity Verification (PIV) credentials, in accordance with National Institute of Standards and Technology (NIST) guidelines, prior to being made operational; or
- 2) upgrade existing PACS and LACS to use PIV credentials in accordance with NIST guidelines, prior to agency using development and technology refresh funds to complete other activities,

All solicitations and contracts that require a contractor to provide one or more of the systems and/or equipment defined in 1004.1302(a) must contain in the requirement that contractor and subcontractor products and services provided in support of the implementation of HSPD-12 are approved as compliant with Federal Information Processing Standards Publication (FIPS PUB) Number 201 and NIST standards (as applicable). The requirement shall specify how the systems

and/or equipment will be used in support of HSPD-12 implementation and require contractors to notify the contracting officer if the statement of work or specification does not conform to FIPS PUB 201 and NIST standards.

For purposes of this section, systems and/or equipment defined in 1004.1302(a) from GSA, Federal Supply Schedule 70, Special Item Number (SIN) 132-62, HSPD-12 Product and Service Components, are approved as compliant with FIPS PUB 201 and NIST standards.

###

Procurement questions regarding this APU may be directed to Michele Sharpe at Michele.Sharpe@treasury.gov. Questions pertaining to HSPD-12 may be directed to Roger Adams, Deputy Executive, Treasury Enterprise Identity, Credential and Access Management (TEICAM) at Roger.Adams@treasury.gov.

cc: Roger Adams

Attachments (2)

M-06-18, Acquisition of Products and Services for Implementation of HSPD-12

M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors.



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

M-06-18

June 30, 2006

MEMORANDUM FOR CHIEF INFORMATION OFFICERS
CHIEF ACQUISITION OFFICERS
CHIEF FINANCIAL OFFICERS

FROM: KAREN EVANS 
ADMINISTRATOR, ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY

ROBERT A. BURTON 
ASSOCIATE ADMINISTRATOR, OFFICE OF FEDERAL
PROCUREMENT POLICY

SUBJECT: Acquisition of Products and Services for Implementation of
HSPD-12

This memorandum provides updated direction for the acquisition of products and services for the implementation of Homeland Security Presidential Directive-12 (HSPD-12) "Policy for a Common Identification Standard for Federal Employees and Contractors" and also provides status of implementation efforts.

Background

HSPD-12 establishes the requirement for a mandatory Governmentwide standard for secure and reliable forms of identification for Federal employees and contractors. As directed by HSPD-12, the National Institute of Standards and Technology (NIST) promulgated Federal Information Processing Standard (FIPS) 201: *Personal Identity Verification of Federal Employees and Contractors* on February 25, 2005. FIPS 201 and associated NIST publications establish standards and requirements for the identity verification of federal employees and contractors and for Personal Identity Verification (PIV) identity credentials to be issued.

OMB policy memorandum M-05-24: *Implementation of Homeland Security Presidential Directive 12* requires federal agencies to deploy products and operational systems to issue identity credentials meeting the FIPS 201 standard by October 27, 2006. The OMB policy memorandum directs that agencies must acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications in order to ensure government-wide interoperability. OMB has designated the General Services Administration (GSA) as the "executive agency for Government-wide acquisitions of information technology to implement HSPD-12." In this capacity, GSA will make approved products and services available through acquisition vehicles that are available to all agencies.

FIPS 201 Product and Service Evaluation and Approval

Both NIST and GSA have established evaluation programs for the testing and evaluation of specific products and services needed for the implementation of HSPD-12. NIST has established the NIST Personal Identity Verification Program (NPIVP) to test and validate Personal Identity Verification (PIV) components and sub-systems required by Federal Information Processing Standard (FIPS) 201. At present, the NPIVP validation program provides for the testing and validation of PIV card applications and PIV middleware for conformance to FIPS 201 and the interface specifications of NIST SP 800-73 *Interfaces for Personal Identity Verification*. NIST has published derived test requirements as NIST SP 800-85A: *PIV Card Application and Middleware Test Guidelines*. All of the tests under NPIVP are handled by third-party test laboratories that are now designated as interim NPVIP Test Facilities. NIST publication FIPS Pub 140-2: *Security Requirements for Cryptographic Modules* also requires the testing and validation of cryptographic modules of PIV cards and other products performing cryptographic functions. This testing is also performed by the accredited third-party facilities designated to perform NPIVP testing. The status and results of these tests and product validation are posted at the NIST NPVIP website: <http://csrc.nist.gov/npivp/>.

GSA also supports the evaluation and approval of products and services required for the implementation of HSPD-12. GSA has identified 21 categories of products/services for which normative requirements are expressed in NIST publication FIPS 201 and associated technical specifications. GSA has established the FIPS 201 Evaluation Program to evaluate and approve such products/services as compliant with specified FIPS 201 requirements. The Evaluation Program also provides for product interoperability and performance testing. Specific evaluation and approval requirements for each of the 21 categories of products/services have been established and publicly posted. Each Approval Procedure cites the specific FIPS 201 requirements that are evaluated for that category of product/service and the type of evaluation needed for approval. The 21 categories of products/services for the FIPS 201 Evaluation Program and Approval Procedures for all 21 of those categories are posted at the FIPS 201 Evaluation Program website: <http://fips201ep.cio.gov/>.

GSA has designated a third-party laboratory for the evaluation and testing of products and services under the FIPS 201 Evaluation Program. Vendors must submit completed application packages and, as appropriate, products if laboratory testing is required.

GSA has established the FIPS 201 Approved Products List for all products and services that have been approved under the GSA FIPS 201 Evaluation Program. To date 49 vendors have enrolled for the Evaluation Program and are in the process of submitting application packages for over 100 products/services across the 21 categories. GSA will continue to evaluate and approve products/services as completed submissions are received; all approved products are posted to the Approved Products List. The Approved Products List can be accessed at: <http://idmanagement.gov>.

There are other types of services that may be necessary for HSPD-12 systems and deployments, but have no normative requirements specified in FIPS 201 and, therefore, are not included in the FIPS 201 Evaluation Program (e.g., integration services, contractor managed services and solutions). Qualification requirements for these services and a list of qualified vendor services are also posted at: <http://idmanagement.gov>.

Acquisition Guidance

GSA has established Special Item Number (SIN) 132-62 on Information Technology (IT) Schedule 70 for the acquisition of approved HSPD-12 Implementation Products and Services. The following categories of services and products are established for SIN 132-62:

1. PIV Enrollment and registration services and products;
2. PIV System infrastructure services and products;
3. PIV Card production services and products;
4. PIV Card activation and finalization services and products;
5. PIV Integration services and products;
6. Logical access control and physical access control services and products;
7. Approved FIPS 201 services and products;
8. Other professional services.

All products and services offered on SIN 132-62 have been evaluated and qualified to be in compliance with government-wide requirements. Agencies may acquire individual product items, deployment services, or complete contractor managed services for any of the HSPD-12 categories or may acquire bundled, integrated solutions. Vendors that are approved to offer contractor managed services for any of the HSPD-12 categories or for complete, integrated solutions are posted at: <http://idmanagement.gov>. The vendors offering contractor managed services for bundled, integrated solutions must ensure that only approved products from the Approved Product List are acquired and incorporated into delivered system solutions.

Agencies may order direct from Schedule 70 SIN 132-62 for all products and services available. Alternatively, the GSA Federal Acquisition Service will support agencies with assisted acquisitions. To engage a Federal Acquisition Service program for support, agencies need to enter an interagency agreement, including establishing a bona fide need with a Federal Acquisition Service program, and transfer funds in accordance with those programs' requirements. GSA has established a cutoff date this year for those agreements of August 30, 2006 for services and September 22, 2006 for supplies.

GSA is also offering Special Item Number 132-61 on GSA IT Schedule 70 for the PKI Shared Service Provider Program. This program provides for approved PKI service providers for the acquisition of PKI certificates and PKI services. The approved PKI Shared Service Providers have been evaluated and determined to be compliant with the requirements of FIPS 201.

Other authentication and identity management service lines for products/services that must be qualified on the basis of common, government-wide requirements will be made available, as required, through additional Special Item Numbers in the SIN 132-**6X** series on GSA IT Schedule 70. Under the Electronic Government Act of 2002, state and local governments may also purchase directly from IT Schedule 70, including Special Item Numbers in the SIN 132-**6X** series.

Agencies that proceed with the acquisition of products and services for the implementation of HSPD-12 through acquisition vehicles other than GSA IT Schedule 70 must ensure that only approved products/services from the Approved Product List are acquired and incorporated into system solutions and ensure compliance with other

federal standards and requirements for systems used to implement HSPD-12. In order to ensure government-wide interoperability, this applies for the lifecycle of the products, services, and/or systems being acquired.

FAR Amendments

The following amendments to the Federal Acquisition Regulation (FAR) are being established:

- FAR Case 2005 015: Common Identification Standard for Contractors. FAR Case 2005 015 applies the identity verification requirements of FIPS 201 to federal contractors. This FAR amendment was published as an interim rule on January 5, 2006 and, following a public comment period, will be issued as a final rule and amendment to the FAR shortly.
- FAR Case 2005 017: Requirement to Purchase Approved Authentication Products and Services. FAR Case 2005 017 requires agencies to acquire only approved PIV products and services. Such products and services may be acquired through GSA IT Schedule 70, SIN 132-62, or if acquired through other acquisition vehicles, agencies must maintain an ongoing plan and ensure products and services acquired conform to all applicable federal standards and requirements for the lifecycle of the components. It is anticipated that this FAR amendment will be issued as a proposed rule shortly.

Attached to this memorandum is a listing of approved products and services and submission status to the FIPS 201 Evaluation Program as of June 30, 2006. Current status information is available at the website: <http://idmanagement.gov>.

Please direct any questions to:

Carol Bales (OMB) 202-395-9915, Carol.A.Bales@omb.eop.gov
David Temoshok (GSA OGP) 202-208-7655, david.temoshok@gsa.gov or
Michel Kareis (GSA FAS) 703-872-3242, michel.kareis@gsa.gov.

Attachment

1. Approved Products and Services for HSPD-12 Implementation

FIPS 201 Evaluation Program Approved Product List

Supplier	FIPS 201 Product/Service Category	Product Identification
Verisign, Inc.	PKI Shared Service Provider	Verisign SSP PKI
Operational Research Consultants, Inc	PKI Shared Service Provider	ORC SSP PKI
Cybertrust, Inc	PKI Shared Service Provider	Cybertrust Federal SSP
Cogent Systems, Inc	Template generator	BioSDK 4.1/COGENT BSP
Cogent Systems, Inc	Template matcher	BioSDK 4.1/COGENT BSP
Cross Match Technologies, Inc	Fingerprint Capture Station	ID 500
Cross Match Technologies, Inc	Fingerprint Capture Station	ID 500M
Cross Match Technologies, Inc.	Fingerprint Capture Station	ID 700
Cross Match Technologies, Inc.	Fingerprint Capture Station	LScan Guardian

Qualified Integration Services

Supplier	HSPD-12 Integration Service Category	Scope
Anteon Corporation	Contractor-managed PIV Integration Services	Complete, end-to-end solution
Lockheed Martin Corporation	Contractor-managed PIV Integration Services	Complete, end-to-end solution
XTec, Inc	Contractor-managed PIV Integration Services	Complete, end-to-end solution

2. Products and Services Applying for Approval

Status	# Total	Status Description
1. # Suppliers Enrolled	49	Total number of suppliers that have enrolled to participate in the FIPS 201 Evaluation Program.
2. # Suppliers initiated Application	29	Total number of suppliers that have initiated the application process for at least one product or service.
3. # Products for which Application has been initiated	109	Total number of products for which suppliers have initiated application process.
4. # Products for which Application Package has been completed.	0	Total number of products for which completed Application Package have been received. Completed packages are necessary to start evaluation process.
5. # Approved Products	9	Total number of approved products with evaluation completed and posted to Approved Product List.



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

THE DIRECTOR

February 3, 2011

M-11-11

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew
Director

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

The *Cyberspace Policy Review*, adopted by the President, and the President’s Budget for Fiscal Year 2011 highlighted the importance of identity management in protecting the nation’s infrastructure. HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials including a standardized background investigation to verify employees’ and contractors’ identities. Specific benefits of the standardized credentials required by HSPD-12 include secure access to federal facilities and disaster response sites, as well as multi-factor authentication, digital signature and encryption capabilities.¹ Additionally, standardization leads to reduced overall costs and better ability to leverage the Federal Government’s buying power with industry.²

As discussed in OMB Memorandum 10-28, “*Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*,” DHS is exercising primary responsibility within the Executive Branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543.

In the attached memorandum, DHS outlines a plan of action for agencies that will expedite the Executive Branch’s full use of the PIV credentials for access to federal facilities and information systems. I ask for your help in overseeing your agency’s implementation of this plan of action and your agency’s completion of its adoption of the PIV credentials.

¹ HSPD-12, paragraph 4, requires that agencies use the identification standard to the maximum extent practicable; therefore, exceptions to using PIV credentials must be due to extenuating circumstances (e.g. system is in the process of being decommissioned.)

² Use of PIV credentials is not required for access to Federal applications where identity assurance is not needed (i.e. E-Authentication Assurance Level 1), such as low risk public-facing websites, blogs, etc. For additional information, refer to NIST Special Publication 800-63 at www.nist.gov.

As the DHS memorandum explains, the majority of the federal workforce is now in possession of the credentials, and therefore agencies are in a position to aggressively step up their efforts to use the electronic capabilities of the credentials. To that end, and as the DHS memorandum further explains, each agency is to develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. Moreover, the DHS memorandum outlines a set of requirements that needs to be included in an agency's implementation policy, in order for that policy to be effective in achieving the goals of HSPD-12 and realizing the full benefits of PIV credentials.

Agency progress on HSPD-12 implementation will be monitored by the National Security Staff, and OMB will continue to provide guidance and oversight for agency Information Technology investments.

Questions for OMB may be directed to Carol Bales at 202-395-9915 or eaauth@omb.eop.gov.

Attachment



February 3, 2011

MEMORANDUM FOR THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Gregory Schaffer, Assistant Secretary for Cyber Security and Communications,
Department of Homeland Security

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

The *Cyberspace Policy Review*, adopted by the President, and the President's Budget for Fiscal Year 2011 highlighted the importance of identity management in protecting the nation's infrastructure. HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials including a standardized background investigation to verify employees' and contractors' identities. Specific benefits of the standardized credentials required by HSPD-12 include secure access to federal facilities and disaster response sites, as well as multi-factor authentication and digital signature and encryption capabilities.¹ Additionally, standardization leads to reduced overall costs and better ability to leverage the Federal Government's buying power with industry.²

This memorandum outlines a plan of action for agencies that will expedite the Executive Branch's full use of the credentials for access to federal facilities and information systems.³ As of December 2010, agencies reported that approximately 5 of 5.7 million federal employees and contractors have completed background investigations, and 4.5 million have PIV credentials. With the majority of the federal workforce now in possession of the credentials, agencies are in a position to aggressively step up their efforts to use the electronic capabilities of the credentials.

To that end, each agency should develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. To be effective in achieving the goals of HSPD-12, and realizing the full benefits of PIV credentials, the agency's policy needs to include the following requirements:

¹ HSPD-12, paragraph 4, requires that agencies use the identification standard to the maximum extent practicable; therefore, exceptions to using PIV credentials must be justified by extenuating circumstances (e.g. system is in the process of being decommissioned.)

² Use of PIV credentials is not required for access to Federal applications where identity assurance is not needed (i.e. E-Authentication Assurance Level 1), such as low risk public-facing websites, blogs, etc. For additional information, refer to NIST Special Publication 800-63 at www.nist.gov.

³ HSPD-12 applies to federal employees and contractors and requires: (1) completion of background investigations; (2) issuance of standardized identity credentials; (3) use of the credentials for access to federal facilities; and (4) use of the credentials for access to federal information systems.

- Effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.⁴
- Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.
- Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation. In order to ensure government-wide interoperability, OMB Memorandum 06-18, “*Acquisition of Products and Services for Implementation of HSPD-12*” requires agencies to acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications.
- Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.⁵
- The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council’s “Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance” (available at www.idmanagement.gov).

As an initial step, I request you designate an agency lead official for ensuring the issuance of the agency’s HSPD-12 implementation policy. Please send the name, title and contact information for your agency’s lead official to HSPD12.FNS@dhs.gov and icam@gsa.gov by February 25, 2011.

The CIO Council guidance referenced above provides agencies with additional guidance to support their HSPD-12 and other identity management implementations. Additional information on HSPD-12 is available in the attached reference materials.

To further support HSPD-12 implementation, the DHS is partnering with the General Services Administration (GSA) on implementation activities. GSA will continue to administer the Interoperability Test Program and Approved Products and Services List for HSPD-12, serve as the Public Key Infrastructure Policy Authority, and manage the HSPD-12 Managed Services Office. The DHS and GSA will work together to provide agencies with guidance for implementing the government-wide architecture defined in the “Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance.” This includes a DHS partnership with the GSA Public Building Service (PBS) to ensure that implementation of physical access requirements for Federal buildings, under PBS’ purview, are implemented in accordance with the

⁴ The Federal Information Security Management Act of 2002 requires agencies to ensure that information security is addressed throughout the life cycle of each agency information system.

⁵ As indicated in paragraph 4 of HSPD-12, agencies were to begin using the common identification standard in November 2006 to gain physical access to federally controlled facilities and logical access to federally controlled information systems.

“Federal Security Level Determinations for Federal Facilities – An Interagency Security Committee Standard” and NIST guidelines.

We welcome any questions your agency might have regarding this guidance. Questions may be directed to HSPD12.FNS@dhs.gov, icam@gsa.gov, or (202) 219-1627. Please share this memorandum with your Chief Information Officers, Chief Information Security Officers, Chief Financial Officers, Chief Human Capital Officers, Chief Privacy Officers, Chief Security Officers, senior agency officials for privacy, senior agency officials for facilities and physical security, budget officers, and any other relevant offices and individuals within your agency.

cc: Howard Schmidt, Special Assistant to the President and Cybersecurity Coordinator,
National Security Staff
Vivek Kundra, Administrator, E-Government and Information Technology, Office of
Management and Budget
Martha N. Johnson, Administrator, General Services Administration

Attachment

References

Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 2004

HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of ID issued by the Federal Government to its employees and employees of federal contractors for access to federally-controlled facilities and networks.

http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

NIST FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors

This standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems except for “national security systems” as defined by 44 U.S.C. 3542(b)(2).

<http://csrc.nist.gov/publications/PubsFIPS.html>

OMB Memorandum 05-24, Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005

This memorandum provides implementing instructions for HSPD-12 and the Standard (NIST FIPS 201.)

<http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2005/m05-24.pdf>

Federal Identity, Credential and Access Management Roadmap and Implementation Guidance

The Federal Identity, Credential, and Access Management (ICAM) Roadmap addresses unclassified federal identity, credential and access management and how the Executive Branch of the Federal Government will interact with external organizations and individuals. It provides a government-wide architecture for ICAM.

<http://www.idmanagement.gov>

NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems

The purpose of this publication is to describe a strategy for agencies to enable their physical access control systems to leverage HSPD-12 Personal Identity Verification (PIV) Credentials. The document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to Federal government facilities and assets.

<http://csrc.nist.gov/publications/nistpubs/800-116/sp800-116.pdf>