PIV-I Requirements

Consolidated from FIPS 201 and OMB M-05-24

#	Ck	Requirement Reference and Text
1		**Part 1#1.** In accordance with HSPD 12, departments and agencies shall meet the requirements of this part no later than eight months following promulgation of the standard.
2		**2.1#1 (b1a).** Credentials shall be issued only to individuals whose true identity has been verified.
3		**2.1#2 (b1b).** Credentials shall be issued only after a proper authority has authorized issuance of the credential.
4		**2.1#3 (b2).** Only an individual with a background investigation on record shall be issued a credential.
5		**2.1#4 (b3).** An individual shall be issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or State government issued picture ID.
6		**2.1#5 (b4).** Fraudulent identity source documents shall not be accepted as genuine and unaltered.
7		**2.1#6 (b5).** A person suspected or known to the government as being a terrorist shall not be issued a credential.
8		**2.1#7 (b6).** No substitution shall occur in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, must be the person to whom the credential is issued.
9		**2.1#8 (b7).** A credential shall not be issued unless it has been requested by proper authority.
10		**2.1#9 (b8).** A credential shall remain serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked.
11		**2.1#10 (b9).** A single corrupt official in the process shall not have the ability to issue a credential with an incorrect identity or to a person not entitled to the credential.
12		**2.1#11 (b10).** An issued credential shall not be [easily] modified, duplicated, or forged
13		**2.2#1 (b1).** The organization shall adopt and use an approved identity proofing and registration process.
14		**2.2#2 (b2a).** The process shall begin with initiation of a National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation required for Federal employment. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI.
15		**2.2#3 (b2b).** The National Agency Check (NAC) shall be completed before credential issuance.
16		**2.2#4 (b2c).** ~~Note: a completed National Agency Check is sufficient for credential issuance; however,~~ The required National Agency Check with Inquiries shall be completed.
17		**2.2#5 (b3).** The applicant must appear in-person at least once before the issuance of a PIV credential.
18		**2.2#6 (b4a).** During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form.
19		**2.2#7 (b4b).** During identity proofing, the identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification.
20		**2.2#8 (b4c).** During identity proofing, at least one document shall be a valid State or Federal government-issued picture identification (ID).
21		**2.2#9 (b5).** The PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.

#	Ck	Requirement Reference and Text
22		**2.2#10.** The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements above and approved in writing by the head of the Federal department or agency.
23		**2.2#11.** A process for registration and approval must be established, using a method approved by the U.S. Department of State's Bureau of Diplomatic Security, for citizens of foreign countries who are working for the Federal government overseas, except for employees under the command of a U.S. area military commander.
24		**2.3#1.** The issuance and maintenance process used when issuing credentials shall be accredited by the department as satisfying the requirements below and approved in writing by the head of the Federal department or agency.
25		**2.3#2 (b1).** The organization shall use an approved PIV credential issuance and maintenance process.
26		**2.3#3 (b2a).** The process shall ensure completion and successful adjudication of a National Agency Check (NAC), National Agency Check with Written Inquiries (NACI), or other OPM or National Security community investigation as required for Federal employment.
27		**2.3#4 (b2b).** The PIV credential shall be revoked if the results of the investigation so justify.
28		**2.3#5 (b3).** The system shall, at the time of issuance, verify that the individual to whom the credential is to be issued (and on whom the background investigation was completed) is the same as the intended applicant/recipient as approved by the appropriate authority.
29		**2.3#6 (b4).** The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited).
30		**2.4#1.** Departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in this standard
31		**2.4#2.** Departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in the E-Government Act of 2002 [E-Gov], as applicable.
32		**2.4#3.** Departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in the Privacy Act of 1974 [PRIVACY], as applicable.
33		**2.4#4.** Departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in Office of Management and Budget (OMB) Memorandum M-03-22 [OMB322], as applicable.
34		**2.4#5.** Departments and agencies may have a wide variety of uses of the PIV system and its components that were not intended or anticipated by the President in issuing [HSPD-12]. In considering whether a proposed use of the PIV system is appropriate, departments and agencies shall consider the aforementioned control objectives and the purpose of the PIV standard, namely "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy." [HSPD-12]
35		**2.4#6.** Departments and agencies shall not implement a use of the identity credential inconsistent with these control objectives.
36		**2.4#7 (b1a).** To ensure the privacy of applicants, departments and agencies shall assign an individual to the role of senior agency official for privacy. The senior agency official for privacy is the individual who oversees privacy-related matters in the PIV system and is responsible for implementing the privacy requirements in the standard.
37		**2.4#8 (b1b).** The individual serving in the role of senior agency official for privacy may not assume any other operational role in the PIV system.

#	Ck	Requirement Reference and Text
38		**2.4$9 (b2a).** To ensure the privacy of applicants, departments and agencies shall conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form for the purpose of implementing PIV, consistent with [E-Gov] and [OMB322].
39		**2.4#10 (b2b).** To ensure the privacy of applicants, departments and agencies shall consult with appropriate personnel responsible for privacy issues at the department or agency (e.g., Chief Information Officer) implementing the PIV system.
40		**2.4#11 (b3a).** To ensure the privacy of applicants, departments and agencies shall write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g., transactional information, personal information in identifiable form [IIF]), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency.
41		**2.4#12 (b3b).** To ensure the privacy of applicants, departments and agencies shall provide PIV applicants full disclosure of the intended uses of the PIV credential and the related privacy implications.
42		**2.4#13 (b4).** To ensure the privacy of applicants, departments and agencies shall assure that systems that contain IIF for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in [PRIVACY].
43		**2.4#14 (b5).** To ensure the privacy of applicants, departments and agencies shall maintain appeals procedures for those who are denied a credential or whose credentials are revoked.
44		**2.4$15 (b6).** To ensure the privacy of applicants, departments and agencies shall ensure that only personnel with a legitimate need for access to IIF in the PIV system are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance.
45		**2.4#16 (b7).** To ensure the privacy of applicants, departments and agencies shall coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system.
46		**2.4#17 (b8).** To ensure the privacy of applicants, departments and agencies shall assure that the technologies used in the department or agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.
47		**2.4#18 (b9).** To ensure the privacy of applicants, departments and agencies shall utilize security controls described in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable. [SP800-53]
48		**2.4#19 (b10).** To ensure the privacy of applicants, departments and agencies shall ~~ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of information in identifiable form. Specifically,~~ employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV credential.
m1		**m0524.1#1** 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.
m2		**m0524.1.A#1** HSPD-12 applies to "executive departments" listed in title 5 U.S.C. § 101.

#	Ck	Requirement Reference and Text
m3		**m0524.1.A#2** HSPD-12 applies to agencies listed in title 5 U.S.C. § 101.
m4		**m0524.1.A#3** HSPD-12 applies to the Department of Homeland Security
m5		**m0524.1.A#4** HSPD-12 applies to "independent establishments" as defined by title 5 U.S.C. §104(1);
m6		**m0524.1.A#5** HSPD-12 applies to United States Postal Service (title 39 U.S.C § 201)
m7		**m0524.1.A#6** HSPD-12 does **NOT** apply to "government corporations" as defined by title 5 U.S.C. § 103(1). (These are encouraged, but not required to implement HSPD-12.)
m8		**m0524.1.B#1** HSPD-12 applies to Federal employees, as defined in title 5 U.S.C § 2105 "Employee," within a department or agency.
m9		**m0524.1.B#2** HSPD-12 applies to individuals employed by, detailed to or assigned to a department or an agency.
m10		**m0524.1.B#3** HSPD-12 applies to, 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).
m11		**m0524.1.B#4** HSPD-12 applies 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) as determined by an agency risk-based decision.
m12		**m0524.1.B#5** HSPD-12 does **NOT** apply to, within DoD and DoS, family members and other eligible beneficiaries.
m13		**m0524.1.B#6** HSPD-12 does **NOT** apply to occasional visitors to Federal facilities to whom departments and agencies would issue temporary identification.
m14		**m0524.1.C#1** HSPD-12 applies to individuals under contract to a department or agency, requiring routine access to federally controlled facilities and/or federally controlled information systems to whom departments and agencies would issue Federal agency identity credentials, consistent with your existing security policies.
m15		**m0524.1.C#2** HSPD-12 does **NOT** apply to individuals under contract to a department or agency, requiring only intermittent access to federally controlled facilities.
m16		**m0524.1.D#1** HSPD-12 applies to 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 HSPD-12.
m17		**m0524.1.D#2** HSPD-12 applies to Federally controlled commercial space shared with non-government tenants. (For example, if a department or agency leased the 10th floor of a commercial building, HSPD-12 applies to the 10th floor only.)
m18		**m0524.1.D#3** HSPD-12 applies to Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.
m19		**m0524.1.D#4** HSPD-12 applies to 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.
m20		**m0524.1.E#1** HSPD-12 applies to information technology system (or information system), as defined by the Federal Information Security Management Act of 2002 (44 U.S.C. § 3502(8)).
m21		**m0524.1.E#2** HSPD-12 applies to 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)).

#	Ck	Requirement Reference and Text
m22		**m0524.1.E#3** HSPD-12 applies to 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) as deemed applicable by a FIPS 199-based risk determination.
m23		**m0524.1.E#4** HSPD-12 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)). (See NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System, 8/03)
m24		**m0524.2.A#1** By 2/25/05, NIST shall publish the HSPD-12 Standard – Federal Information Processing Standard 201 (FIPS 201).
m25		**m0524.2.A#2** By 6/25/05, NIST shall release the technical reference implementation.
m26		**m0524.2.A#3** By 8/5/05, NIST shall release conformance testing information.
m27		**m0524.2.B#1** By 6/27/05, departments and agencies shall submit implementation plans to OMB.
m28		**m0524.2.B#2** By 8/26/05, departments and agencies shall provide list of other potential uses of FIPS 201 (see question 7).
m29		**m0524.2.B#3** By 10/27/05, departments and agencies shall comply with FIPS 201, Part 1 (see question 3).
m30		**m0524.2.B#4** By 10/27/06, departments and agencies shall begin compliance with FIPS 201, Part 2 (see question 4).
m31		**m0524.2.B#5** By 10/27/07, departments and agencies shall verify and/or complete background investigations for all current employees *who have been Federal department or agency employees 15 years or less* and contractors (see question 3).
m32		**m0524.2.B#6** By 10/27/08, departments and agencies shall complete background investigations for all Federal department or agency employees employed over 15 years (see question 3).
m33		**m0524.2.B#7** By 7/31/05, GSA shall establish authentication acquisition services (see question 5)
m34		**m0524.2.B#8** By 10/27/05, GSA shall sponsor Federal Acquisition Regulation (FAR) amendment implementing FIPS 201
m35		**m0524.3.A#1** By 10/27/05 - for all new employees, contractors and other applicable individuals - departments and agencies must adopt and accredit a registration process consistent with the identity proofing, registration and accreditation requirements in section 2.2 of FIPS 201 and NIST Special Publication 800-79: *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, regardless of whether the department or agency will be ready to issue standard compliant identity credentials by October 27, 2005.
m36		**m0524.3.A#2** This registration process will apply to all new identity credentials issued to any new employees, contractors or other applicable individuals (i.e. no new identity credentials can be issued until these conditions are met).
m37		**m0524.3.B#1** By 10/27/05 - for all new employees, contractors and other applicable individuals - departments and agencies must initiate the National Agency Check with Written Inquiries (NACI) or other suitability or national security investigation prior to credential issuance.
m38		**m0524.3.B#2** By 10/27/05 - for all new employees, contractors and other applicable individuals - departments and agencies must receive notification of results of the National Agency Checks before issuing the credential *within the first 5 days* of NAC submission. [I.e., all National Agency Checks – (a) Security/Suitability Investigations Index (SII), (b) Defense Clearance and Investigation Index (DCII), (c) FBI Name Check, and (d) FBI National Criminal History Fingerprint Check – must complete and be received before a PIV Card can be issued within the first 5 days of NAC submission.]

#	Ck	Requirement Reference and Text
m39		**m0524.3.B#3** By 10/27/05 - for all new employees, contractors and other applicable individuals - departments and agencies must receive notification of results of the FBI National Criminal History Check (fingerprint check) before issuing the credential *after the first 5 days* of NAC submission. [Section 2.2 of FIPS 201 has been revised to clarify for the initial credential issuance, only the fingerprint check must be completed.]
m40		**m0524.3.B#4** By 10/27/05 - for all new employees, contractors and other applicable individuals - departments and agencies must ensure that 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.
m41		**m0524.3.B#5** By 10/27/05 - for all new employees, contractors and other applicable individuals - departments and 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.
m42		**m0524.3.B#6** By 10/27/05 - for all new employees, contractors and other applicable individuals - departments and agencies must, since Foreign National employees and contractors may not have lived in the United States long enough for a NACI to be meaningful, conduct an equivalent investigation, consistent with their 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.]
m43		**m0524.3.C#1** By 10/27/05 ~~- for all new employees, contractors and other applicable individuals -~~ departments and agencies must include language implementing FIPS 201 in applicable new contracts.
m44		**m0524.3.C#2** By 10/27/05 ~~- for all new employees, contractors and other applicable individuals - departments and agencies must~~ 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 HSPD-12 and FIPS 201 for affected contractor personnel.
m45		**m0524.3.C#3** By 10/27/05 ~~- for all new employees, contractors and other applicable individuals -~~ departments and agencies must comply with the forthcoming Federal Acquisition Regulation sections on these requirements.
m46		**m0524.3.D#1** By 10/27/05 - for current employees - departments and agencies must 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.
m47		**m0524.3.D#2** By 10/27/07 - for current employees *who have been Federal department or agency employees 15 years or less* - departments and agencies must verify and/or complete background investigations.
m48		**m0524.3.D#3** By 10/27/05 - for current employees - departments and agencies must follow NACI requirements at card renewal (every 5 years) 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).]
m49		**m0524.3.D#3** By 10/27/08 - for current employees who have been Federal department or agency employees over 15 years - departments and agencies must verify and/or complete background investigations. [A new investigation may be delayed past 10/27/07, commensurate with risk, but must be completed no later than 10/27/08.]

#	Ck	Requirement Reference and Text
m50		**m0524.3.E#1** By 10/27/05 - for current contractors and other applicable individuals - departments and agencies must develop a plan and begin the required background investigations for all current contractors who do not have a successfully adjudicated investigation on record.
m51		**m0524.3.E#2** By 10/27/07- for current contractors and other applicable individuals - departments and agencies must phase in ~~this requirement~~ background investigations where there is not a successfully adjudicated investigation on record. [Phase in this requirement to coincide with the contract renewal cycle, but no later than 10/27/07.]
m52		**m0524.4.A#1** By 10/27/06, all departments and agencies must issue and require the use of identity credentials for all new employees and contractors, compliant with Parts 1 and Part 2 of FIPS 201.
m53		**m0524.4.A#2** By 10/27/07, all departments and agencies must issue and require the use of identity credentials to all current employees and contractors, compliant with Parts 1 and Part 2 of FIPS 201.
m54		**m0524.4.B#1** By 10/27/06, all departments and agencies must implement the technical requirements of FIPS 201 in the areas of personal authentication, access controls and card management, consistent with FIPS 201 (i.e. sections 3, 4, and 5) and NIST Special Publication 800-73.
m55		**m0524.4.C#1** By 10/27/06, for facility access, all departments and agencies must use the appropriate card authentication mechanism described in section 6 of FIPS 201, with minimal reliance on visual authentication to the maximum extent practicable (section 6.2.1).
m56		**m0524.4.C#2** By 10/27/06, for facility access, all departments and agencies must have officials who control access determine the appropriate card authentication mechanism based on risk determinations.
m57		**m0524.4.D#1** By 10/27/06, all ~~departments and agencies must~~ mandatory and 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. (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.)
m58		**m0524.4.D#2** By 10/27/06, all departments and agencies must require the use of the identity credential for system access.
m49		**m0524.4.D#3** By 10/27/06, all departments and agencies must prioritize this requirement [for the use of the identity credential for system access] based on risk, using authentication risk assessments required by OMB Memorandum M-04-04 (E-Authentication Guidance for Federal Agencies, 12/16/03, www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf) and the categorization required by FIPS 199. (Standards for Security Categorization for Federal Information and Information Systems, 2/04, www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf) Document the results and make available to your Chief Information Officer, security office and Inspector General's Office upon request.
m60		**m0524.4.D#4** By 10/27/06, all departments and agencies must document the results of the prioritization based on risk and make available to their Chief Information Officer, security office and Inspector General's Office upon request.
m61		**m0524.4.D#5** By 10/27/06, all departments and agencies must provide all employees and contractors with access to documentation regarding rules of behavior (including the consequences for violation) for system access. [Departments and agencies are already required to have rules of behavior in place. See OMB Circular A-130, www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf]

#	Ck	Requirement Reference and Text
m62		**m0524.5.A#1** [To ensure government-wide interoperability,] All departments and agencies must acquire products and services that are approved to be compliant with FIPS 201 and included on the approved products list. A forthcoming Federal Acquisition Regulation will require the use of only approved products and services**.**
m63		**m0524.5.B#1** [Info only, not a requirement.] 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.
m64		**m0524.5.B#2** 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.
m65		**m0524.5.B#3** Any agency making procurements outside of GSA vehicles for approved products must ensure interoperability and conformance to applicable federal standards for the lifecycle of the components.
m66		**m0524.5.B#4** Any agency making procurements outside of GSA vehicles for approved products must maintain a written plan for ensuring ongoing conformance to applicable federal standards for the lifecycle of the components.
m67		**m0524.6.A** Prior to identification issuance, departments and agencies must ensure personal information collected for employee and contractor identification purposes is handled consistent with the Privacy Act of 1974 (5 U.S.C. § 552a).
m68		**m0524.6.B** Prior to identification issuance, departments and agencies must assign an individual to be responsible for overseeing the privacy-related matters associated with implementing HSPD-12.
m69		**m0524.6.C#1** Prior to identification issuance, departments and agencies must submit a comprehensive privacy impact assessment (PIA) of their HSPD-12 program to OMB.
m70		**m0524.6.C#2** Prior to identification issuance, departments and agencies must make their HSPD-12 program PIA publicly available.
m71		**m0524.6.C#3** Departments and agencies must include in their HSPD-12 program PIA analysis of the information technology systems used to implement HSPD-12.
m72		**m0524.6.C#4** The HSPD-12 program PIA must comply with section 208 of the E-Government Act of 2002 (44 U.S.C. ch. 36)
m73		**m0524.6.C#5** The HSPD-12 program PIA must comply with OMB Memorandum M-03-22 of September 26, 2003, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002."
m74		**m0524.6.C#6** Departments and agencies must periodically review and update their HSPD-12 program PIA.
m75		**m0524.6.C#7** Departments and agencies must email their completed PIA to pia@omb.eop.gov.
m76		**m0524.6.D#1** Prior to identification issuance departments and agencies must 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 (www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf).

#	Ck	Requirement Reference and Text
m77		**m0524.6.D#2** These SORNs should be periodically re-reviewed to ensure accuracy.
m78		**m0524.6.E#1** Departments and agencies must collect information using only forms approved by OMB under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. ch. 35), where applicable.
m79		**m0524.6.E#2** Departments and agencies are encouraged to use Standard Form 85, Office of Personnel Management Questionnaire for Non-Sensitive Positions (OMB No. 3206-0005) or Standard Form 85P, Office of Personnel Management Questionnaire for Positions of Public Trust (OMB No. 3206-0005) when collecting information.
m80		**m0524.6.E#3** Departments and agencies, if they plan to collect information from individuals covered by the PRA using a new form, must obtain OMB approval of the collection under the PRA process.
m81		**m0524.6.F** Prior to identification issuance, departments and agencies must develop, implement and post in multiple locations (e.g., agency intranet site, human resource offices, regional offices, provide at contractor orientation, etc.) the 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.
m82		**m0524.6.G#1** Prior to identification issuance, departments and agencies must adhere to control objectives in section 2.1 of FIPS 201. Any uses of the credential not intended or anticipated by HSPD-12 must be appropriately described and justified in your SORN(s) and PIA.
m83		**m0524.7.A#1** Departments and agencies must respond to Paragraph 5 of HSPD-12 - "identify those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of FIPS 201 in circumstances not covered by HSPD-12 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 FIPS 201 not meeting the control objectives listed in FIPS 201.
m84		**m0524.7.A#2** Departments and agencies should submit any identified "other facilities, information systems or applications" 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.
m85		**m0524.7.B** Departments and agencies must report annually 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 FIPS 201). Future OMB guidance will address this requirement.
m86		**m0524.7.C** [not a requirement.] Departments and agencies may defer the capture of biometrics for the identity credential until the NIST guidance is final. [NIST Special Publication 800-76: Biometric Data Specifications for Personal Identity Verification]
m87		**m0524.7.D** Departments and agencies with employees who serve undercover shall implement HSPD-12 in a manner consistent with maintenance of the cover, and to the extent consistent with applicable law and policy.
m88		**m0524.7.E** 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 HSPD-12.

#	Ck	Requirement Reference and Text
m89		**m0524.7.F#1** For temporary personnel employed 6 months or greater, departments and agencies must apply all sections of this guidance, including the background investigation requirements in FIPS 201 (e.g. "completed National Agency Check with Written Inquires [NACI] or other Office of Personnel Management or National Security community investigation").
m90		**m0524.7.F#2** For temporary personnel employed 6 months or less, departments and agencies must apply adequate controls to systems and facilities (i.e. ensuring temporary staff has limited/controlled access to facilities and information systems).
m91		**m0524.7.F#3** For temporary personnel employed 6 months or less, departments and agencies must 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.
m92		**m0524.7.F#4** For temporary personnel employed 6 months or less, departments and agencies must document any security violations involving these employees, and report them to the appropriate authority within 24 hours.
m93		**m0524.7.F#5** For temporary personnel employed 6 months or less, departments and agencies must issue identity credentials to these individuals that are visually and electronically distinguishable from identity credentials issued to individuals to whom FIPS 201 does apply.
m94		**m0524.7.F#6** For temporary personnel employed 6 months or less, departments and agencies should be careful not to develop policies which overlap or contradict FIPS 201's processes for identity proofing and issuance.
m95		**m0524.6.E#7** For occasional visitors, departments and agencies must apply adequate controls to systems and facilities (i.e. ensuring visitors have limited/controlled access to facilities and information systems).
m96		**m0524.6.E#8** For occasional visitors, departments and agencies must develop agency-specific visitor policies (as appropriate).