

HSPD-12 FAQs – October 1, 2009

POLICY

1. Are waivers to the standard allowed?

There is no provision for waivers to standards issued by the Secretary of Commerce under the Federal Information Security Management Act of 2002. HSPD 12 also does not provide a waiver provision.

2. Is it OMB's and NIST's intent that agencies conduct investigations on and issue PIV/smart cards to large numbers of construction contractors (e.g., brick layers, plumbers, welders, etc.) who are responsible for construction of buildings on federal property, where the construction time exceeds 6 months?

OMB Memorandum 05-24 indicates that contractors will need badges if they will be routinely accessing government facilities and/or IT Systems on a regular basis for a period in excess of 6 months. It is up to the employing agency whether any particular contractor employee fulfills these criteria and must therefore be put through the FIPS-201 badging process. (Ref: OMB M-05-24 Sections 1.C, 7.F)

3. How is agency compliance monitored and what happens if an agency does not comply?

Like many other agency activities, oversight is the responsibility of each agency, the Office of Management and Budget, the Government Accountability Office, and oversight committees of Congress. NIST is responsible for providing a conformance test program to help agencies comply with FIPS 201. Information on the conformance program is available at <http://csrc.nist.gov/piv-program>. Non-compliance may include a range of consequences from negative audit reports to budgetary impacts. More importantly, agencies that do not comply will not meet the President's goals of secure and reliable identification for federal employees and contractors.

4. What are the funding sources for agency implementation of FIPS 201?

All federal agencies have existing background investigation, access control, and identification credential activities. It is anticipated that these activities, and the funding used to support them will be used in support of activities compliant with FIPS 201. Any additional funding needs for implementing FIPS 201 should be requested by agencies through the normal federal budget process.

5. If there are employees and contractors working for another Federal agency working on contracts or services that support the tenant agency, can a PIV be issued by the agency whose property they work on or does the PIV have to be issued by the employing agency. Example: GSA provided maintenance support working in the building but the GSA office is not on site.

The authorization for card issuance should originate with the employing agency (or contracting agency in the case of contractors). However, there is nothing to prohibit one agency from providing issuance services to another agency in accordance with interagency MOA/MOU.

6. Does HSPD-12 require that a PIV credential be issued before a new employee is granted any access to Federal facilities or information systems?

No. Agencies may, at their discretion, issue new employees temporary ID badges for access while PIV enrollment and card issuance is in process. These temporary badges must be physically and electronically distinguishable from PIV credentials.

7. Can a PIV card be used by other organizations for other purposes (e.g., access to private facilities, identification for airline travel)?

HSPD-12 and FIPS-201 do not impose any restrictions on the use of the PIV card as an identity credential.

8. Is a Special Agreement Check (SAC) necessary or recommended in order to fulfill the FIPS 201 investigative mandate?

No. The investigative requirements set forth in FIPS 201 state: "...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..." A SAC investigation will not meet the requirements of FIPS 201.

9. Can agencies use other investigative service providers in lieu of OPM to conduct the investigations required by FIPS 201?

No, unless an agency has original or OPM delegated authority to conduct background investigations. Contractor investigations must follow FIPS 201 and agency employee investigation processes.

10. Must reinvestigations be conducted to keep PIV credentials valid?

Currently, PIV credentials do not require reinvestigations to remain valid. Agencies must, however, continue to comply with the reinvestigative requirements set forth by OPM.

11. Do fingerprints used for the National Criminal History Check (NCHC) need to be taken during the PIV enrollment action?

If HSPD-12 applies, then yes, agencies must ensure full compliance with FIPS 201 Section 4.4.1, particularly the requirement that fingerprints taken during the PIV enrollment action "shall be used for one-to-many matching with the database of fingerprints maintained by the FBI." This ensures that fingerprints taken during the same enrollment action are used for the PIV Card templates and the FBI National Criminal History Check of the PIV applicant.

12. If a person has had a "break in service" (i.e., left a job for which they had to be investigated to meet FIPS 201 requirements), must a new investigation be conducted for that person to receive a new PIV credential?

If the "break in service" is two years or more, a new investigation must be conducted before a PIV credential can be issued. In accordance with Executive Order 12968, if the break in service is less than two years, an updated security questionnaire should be completed and any admitted issues resolved as appropriate.

13. If there is a NACI on record that is over 15 years old, does a new NACI have to be submitted?

While there is no requirement for NACIs to be renewed, there must be a record on file indicating employees and contractors have completed at least the minimum background check requirements. If an employee or contractor completed the NACI process and records cannot be located then the individual would need to undergo the NACI (or equivalent) process again.

Note that many employees and contractors will have background checks superior to a NACI (e.g. LBI) and in this case the individuals would not need to complete the NACI process as long as there is a record the investigative requirements were met.

An exception to the above requirements is when there is a break in service of over two years. In this case, an individual would need to undergo a new background check.

14. Can a National Agency Check with Law and Credit (NACLC) be used for PIV credential issuance?

The NACLC is often used as the minimum investigative requirement for access to Secret information and below for military service personnel and Federal contractors. For purposes of PIV credential issuance, the NACLC satisfies the essential requirements.

15. How do I verify whether or not a NACI (or equivalent) has already been completed on an existing employee or contractor?

Authorized personnel security offices may get this information directly from the OPM investigations database. If an agency's personnel security office does not have access, they should contact OPM's Agency Liaison Group at 703-603-0442. Additionally, older "Official Personnel Folders" contain SF-86s and SF-171s bearing a stamp which usually reads "Investigated to 10450 standards". Agencies may take this as evidence a NACI was completed".

16. Is there a point of contact for Joint Personnel Adjudication System (JPAS) and Scattered Castles that non-DoD agencies can contact?

For JPAS inquires, you may contact Juana Smith 703-325-9495 or Steve Long 703-325-6062. For Scattered Castles inquires, you may contact the ODNI Special Security Center (SSC) Help Desk on 1-866-304-4238 or dni-ssc-help@ugov.gov.

17. For the PKI Credentials, are Registration Practices Agreements, additional Certificate Policies, or other methods of qualifying certificates use supported/encouraged/discouraged?

FIPS 201 and the Common Policy do not prohibit inclusion of additional certificate policies, (non-critical) private extensions, or extended key usage OIDs in the certificates. An agency can add whatever local information they need to the certificate; the agency cannot count on relying parties outside of the agency to recognize or honor that information. The Federal Common Policy Framework has been provided as a standard trust anchor for FIPS-201 implementation. When reliance on a certificate is required or optionally chosen, Federal Relying Parties are expected to employ due diligence in tracing the certificate 'path' to ensure the credential can be trusted, e.g. it uses the Common Policy Framework as its trust anchor. It is an Information Technology Security responsibility to ensure the relying party application is properly configured to accept or reject credentials based on these trust relationships. (Ref: OMB M-05-24, Section 4.D).

For questions on HSPD 12 policy, you may contact Carol Bales, OMB Senior Policy Analyst, on 202-395-9915.