UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

July 31, 2008

MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES

FROM: LINDA M. SPRINGER
DIRECTOR

SUBJECT: Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12

This memorandum provides final government-wide credentialing standards to be used by all Federal departments and agencies in determining whether to issue or revoke personal identity verification (PIV) cards to their employees and contractor personnel, including those who are non-United States citizens. These standards replace the interim standards issued in December 2007. The authority is section 2.3(b) of Executive Order 13467 of June 30, 2008.[1]

In addition to the requirements in this memorandum, credentialing determinations are also subject to the requirements of Homeland Security Presidential Directive (HSPD) 12 and issuances developed by the National Institute of Standards and Technology (NIST) and OMB.[2]

HSPD-12 Credentialing Standards

The purpose of this section is to provide minimum standards for initial eligibility for a PIV card. If an individual who otherwise meets these standards is found: 1) unsuitable for the competitive civil service under 5 CFR part 731, 2) ineligible for access to classified information under E.O. 12968, or 3) disqualified from appointment in the excepted service or from working on a contract, the unfavorable decision is a sufficient basis for non-issuance or revocation of a PIV card.

[1] The authority for the interim guidance was a June 1, 2007 delegation by the Office of Management and Budget (OMB) for the U.S. Office of Personnel Management (OPM) to develop adjudication policy for PIV cards under a framework jointly established by OPM and the National Security Council. In the June 30, 2008 Executive Order, however, the President conferred upon OPM the continuing responsibility "for developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient and timely completion of investigations and adjudications relating to . . . eligibility for logical and physical access" to federally controlled facilities or information systems (other than occasional or intermittent access). Accordingly, OPM's authority to issue these standards is now a direct delegation from the President.

[2] NIST FIPS 201-1, March 2006; OMB Memorandum M-05-24, August 2005.

A PIV card will not be issued[3] to a person if:

1. The individual is known to be or reasonably suspected of being a terrorist[4];

2. The employer is unable to verify the individual's claimed identity;

3. There is a reasonable basis to believe[5] the individual has submitted fraudulent information concerning his or her identity;

4. There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;

5. There is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately; or

6. There is a reasonable basis to believe the individual will use Federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

Supplemental Credentialing Standards

Many departments and agencies work with individuals who do not require a suitability determination or a security clearance. In such cases, agencies have the flexibility to apply supplemental credentialing standards in addition to the six basic standards above.[6] The supplemental standards are intended to ensure that the grant of a PIV card to an individual does not create unacceptable risk, when the individual is not subject to an adjudication of suitability for employment in the competitive service under 5 CFR part 731, of qualification for employment in the excepted service under 5 CFR part 302 or under a similar authority, or of eligibility for access to classified information under E.O. 12968. These standards may be applied based on the risk associated with the position or work on the contract.

---

[3] Refer to section 2.1 of FIPS 201-1 for additional instructions on the issuance of PIV cards.

[4] OPM's background investigation includes checking names against the FBI's investigation files.

[5] A reasonable basis to believe occurs when a disinterested observer, with knowledge of the same facts and circumstances, would reasonably reach the same conclusion. Departments and agencies should consult with their legal counsel about any legal questions concerning the standards.

[6] Agencies may have unique specific categories of individuals such as guest researchers, volunteers, or intermittent, temporary, or seasonal employees. OMB Memorandum M-05-24, August 2005 directs that these credentialing standards generally apply to such categories unless they are short-term (i.e. less than 6 months) employees, in which case the agency has discretion based on risk and other factors.

A department or agency may consider denying or revoking a PIV card to an individual based on one of these supplemental credentialing standards.[7] In the following standards, an "unacceptable risk" refers to an unacceptable risk to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial, or medical records; or to the privacy of data subjects.

1. There is a reasonable basis to believe, based on the individual's misconduct or negligence in employment, that issuance of a PIV card poses an unacceptable risk;

2. There is a reasonable basis to believe, based on the individual's criminal or dishonest conduct, that issuance of a PIV card poses an unacceptable risk;

3. There is a reasonable basis to believe, based on the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of a PIV card poses an unacceptable risk;

4. There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

5. There is a reasonable basis to believe, based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

6. A statutory or regulatory bar prevents the individual's contract employment; or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of a PIV card poses an unacceptable risk; or

7. The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

Credentialing Process

OMB's guidance and FIPS 201-1 require that departments and agencies initiate a background investigation (NACI or at least equivalent) and ensure the FBI fingerprint check is completed before issuing an identity credential. Consequently, departments and agencies should begin the credentialing process at least as soon as a person accepts an offer of employment. This may be done by authorizing the person to complete the appropriate investigation forms on-line through

[7] Although some of these factors may be similar to factors considered in making suitability determinations for competitive service employment, see 5 CFR part 731, the determinations being made are not suitability determinations and the procedures to be applied are the procedures laid out in HSPD-12 and guidance issued thereunder, not procedures that apply to suitability determinations or suitability actions.

OPM's e-QIP application site. Departments and agencies are to apply the HSPD-12 credentialing standards set forth above to determine whether the results of a person's background investigation support the grant, denial or revocation of a PIV card. The PIV credentialing process does not interfere with department or agency discretion to make suitability or national security (security clearance) determinations either before or after a person has entered on duty.

Please note that Departments and agencies must verify employment authorization of all new Federal hires with the Department of Homeland Security (DHS) in accordance with OMB Memorandum 07-21, *Verifying the Employment Eligibility of Federal Employees.*[8] When credentialing for new Federal hires, departments and agencies should confirm that a query was conducted through the E-Verify system operated by the U.S. Citizenship and Immigration Services (USCIS).[9]

Departments and agencies may issue credentials using one of the following options:

Option 1--Interim credentialing determination followed by a final credentialing determination:

When a department or agency wishes to bring a new employee or contract employee[10] on board pending completion of a background investigation or any applicable suitability and/or national security decision under 5 CFR part 731 and EO 12968 respectively, or any decision as to whether an individual is qualified for an excepted service appointment or to work on a contract, the department or agency may first make an interim credentialing determination. The interim credentialing determination must be based on:

A. The person presenting two identity source documents, at least one of which is a valid Federal or State government-issued picture identification, and

B. A National Agency Check (NAC) or an FBI National Criminal History Check (fingerprint check).

Upon completion of a background investigation, and at the time of a determination of suitability for an appointment in the competitive service under 5 CFR part 731, eligibility for access to classified information under E.O. 12968, or qualification for an appointment in the excepted service or to work on a contract, a department or agency should simultaneously make a final credentialing determination.

---

[8] For additional information on USCIS' E-Verify program, please call 1-888-464-4218 or visit www.uscis.gov/E-Verify.

[9] If the PIV process identifies that an E-Verify query has not been conducted on a Federal employee hired after the hiring agency's enrollment in the program, that omission in the hiring process should be corrected by the agency by initiating the query as soon as possible.

[10] Credentialing requirements also apply to other categories of individuals being brought on board and identified by agencies as requiring PIV credentials.

Option 2—Single and final credentialing determination before employment:

A department or agency may decide to issue a PIV card only after a single and final credentialing determination is made based on a completed background investigation, or after any applicable determination of suitability for an appointment in the competitive service under 5 CFR part 731, eligibility for access to classified information under E.O. 12968, or qualification for an appointment in the excepted service or to work on a contract, is made on the same person.

Reconsideration (Appeal) Process

FIPS 201-1 requires that each department and agency establish a reconsideration (appeal) process to review requests by persons who have been denied a PIV card or have had their PIV cards revoked by that agency. The precise content of such reconsideration processes is left to the discretion of each agency or department. However, no reconsideration is required when the department or agency denies a PIV card based on the results of a negative suitability determination under 5 CFR part 731 or a decision to deny or revoke a security clearance. In those situations, the reconsideration process does not apply because the person is already entitled to seek review under applicable suitability or national security procedures. Likewise, there is no right to reconsideration in those situations where the department or agency denies a PIV card based on the results of a determination to disqualify the person from an appointment in the excepted service or from working on a contract.

The reconsideration process is final and there is no further right of review.

Reciprocity of Credentialing Determinations

OMB guidance requires agencies to accept PIV card credentialing determinations for a person transferring from another department or agency when the possession of a valid Federal identity credential can be verified by the person's former department or agency and the individual has undergone the required NACI or other suitability or National Security investigation at the person's former department or agency.[11] Beginning in 2009, agencies will record in CVS whether the person received a PIV card and its investigative basis (e.g. NACI).[12]

At a department or agency's discretion, a person may be ineligible for a PIV card when the former employing department or agency (1) determined he or she is unsuitable for employment in the competitive service under 5 CFR part 731, (2) denied (or revoked) his or her security clearance under E.O. 12968, or (3) disqualified him or her from an appointment in the excepted service or from working on a Federal contract. Credentialing determinations are maintained by the granting agency in its Identity Management System (IDMS) and the agency also provides the

[11] For reciprocity in the case of non-U.S. nationals, please see the final paragraph under the section entitled "Credentialing of non-United States Nationals."

[12] This capacity for CVS is currently in the final development phase and is slated for introduction by October 1, 2008. OPM will provide information to agencies on utilizing this capability.

data to CVS for reciprocity purposes. This will allow agencies to certify to each other the HSPD-12 credentialing of employees and contractor personnel.

If a person's eligibility for a PIV card is unfavorably adjudicated for reasons other than standards 1-6 of the basic HSPD-12 Credentialing Standards, and the person is subsequently determined to be suitable, granted a clearance, qualified for appointment in the excepted service or qualified to work on a Federal contract, the department or agency should simultaneously make a new credentialing determination.

Privacy Protection/Records Management

FIPS 201-1 requires that departments and agencies ensure the privacy of applicants for identity credentials and ensure that PIV cards are used solely "to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy."

The credentialing process used by departments and agencies must follow Federal privacy laws and policies as well as the requirements for privacy protection and records management outlined in the NIST issuances concerning credentialing (e.g., FIPS 201-1).

Credentialing of non-United States Nationals

Departments and agencies are required to apply the above credentialing process and standards to non-U.S. nationals[13] who work as employees or contractor employees for Federal departments or agencies and may include others who require long-term logical or physical access to Federal government facilities whether overseas or in the United States. However, special considerations apply to non-U.S. nationals.

At U.S.-Based Locations and in U.S. Territories (Other than American Samoa and Commonwealth of the Northern Mariana Islands (CNMI)[14]:

Departments and agencies must verify employment authorization of new Federal employees with the Department of Homeland Security (DHS) in accordance with OMB Memorandum 07-21, *Verifying the Employment Eligibility of Federal Employees.*

For individuals who are non-U.S. nationals in the United States or U.S. territory for 3 years or more a background investigation (i.e. NACI or equivalent) must be initiated after employment

---

[13] The term "United States national" includes both U.S. citizens and U.S. non-citizen nationals (i.e., American Samoans).

[14] The U.S. territories of American Samoa and CNMI are not included in the "United States" as defined by the Immigration and Nationality Act, and therefore the DHS E-Verify and SAVE verification programs are unable to verify work authorization or immigration status of individuals in those locations. Agencies should conduct such background investigation as may be possible and appropriate under the circumstances in these territories. Recent legislation (Public Law 110-229) will phase-in U.S. immigration law to the CNMI in the future but this has not yet occurred.

authorization is appropriately verified through E-Verify (or immigration status is appropriately verified for those individuals not working for the Federal Government through the USCIS' Systematic Alien Verification for Entitlements (SAVE) system).[15]

For non-U.S. nationals in the U.S. or U.S. territory for less than three years, agencies may delay the background investigation until the individual has been in the U.S. or U.S. territory for three years. In such cases, an alternative facility access identity credential may be issued at the discretion of the relevant agency official as appropriate based on a risk determination. Before an alternative identity credential may be issued, the individual's employment authorization must be verified and an FBI fingerprint based criminal history must be completed If the agency decides to delay the background investigation, the agency must request an FBI Investigations Files (name check search), a name check against the Terrorist Screening Database, and a USCIS Check against SAVE.

Agencies may also choose to include additional checks as appropriate. Furthermore, agencies may establish a Special Agreement Check (SAC) with OPM for the purpose of conducting the FBI fingerprint based criminal history check and other national agency checks on non-U.S. nationals. Please contact the Agency Liaison Group (ALG) with OPM's Federal Investigative Services Division (FISD) at (703) 603-0442.

At Foreign Locations:

Departments and agencies must initiate and ensure the completion of a background investigation before applying the credentialing standards. However, the type of background investigation may vary based on standing reciprocity treaties concerning identity assurance and information exchange that exist between the United States and its Allies or agency agreements with the host country. In most cases OPM will not be able to conduct a NACI, unless the non-U.S. national is or has been residing in the United States.

The background investigation must be consistent with a NACI to the extent possible and include a fingerprint check against the FBI criminal history database, an FBI Investigations Files (name check search), and a name check against the Terrorist Screening Database. Agencies may also choose to include additional checks as appropriate.

As in the United States, for those non-U.S. nationals where a NACI or equivalent cannot be performed, an alternative facility access identity credential may be issued at the discretion of the Department of State Chief of Mission Authority, Department of Defense Installation Commander, and/or other agency official as appropriate based on a risk determination.

Whether at a U.S.-based or foreign location, reciprocity between agencies is not mandatory in the case of alternative identity credentials issued to non-U.S. nationals. Agencies may choose to honor such credentials from other agencies, but that is at their discretion.

---

[15] For additional information about USCIS's SAVE program, please call 1-888-464-4218.

Further Information

For additional information or if you have questions about the HSPD-12 credentialing standards or the credentialing process, please contact the Operational Policy Group, Federal Investigative Services Division, OPM at 202-606-1042.