

## **Attachment #2**

### **Contractor Personnel Security Requirements March 1, 2011**

Reference:

VHA Directive 0710, Personnel Security and Suitability Program/ May 18, 2007

VA Handbook 0710, Personnel Suitability and Security Program/ September 10, 2004

Upon contract award, all key personnel shall be subject to the appropriate type of background investigation or screening per VA/VHA directive 0710 and must receive a favorable adjudication from CCA Personnel Security Specialist or VA Security and Investigations Center (SIC) depending on investigation or screening required. This requirement is applicable to all subcontract personnel. If the investigation or screening is not completed prior to the start date of the contract, the Contractor will be responsible for the actions of those individuals they provide to perform work for VA.

Contract personnel who previously received a favorable adjudication as a result of a Government background investigation or screening may be exempt from this contract requirement. They must provide documentation to support the previous adjudication. Proof of previous adjudication must be submitted by the Contractor to the VA Contracting Officer. Proof of previous adjudication is subject to verification. Some positions may be subject to periodic re-investigation/screening.

1. Position Risk/Sensitivity – For all positions required under this contract, the position risk/sensitivity has been designated as: **Low Risk**
2. Background Investigation/Screening – It is anticipated that the Contractor or contract personnel will be providing services at a VA facility(s) for MORE than 180 days under a single contract or series of contracts, or have access to VA computer data systems. The background investigation/screening commensurate with the requirements of this contract is: **NACI**
3. Contractor Responsibilities
  - a. The Contractor shall prescreen all personnel to ensure they are able to read, write, speak, and understand the English language.
  - b. The Contractor shall submit or have their contract personnel submit the following required forms to the Personnel Security Specialist or VA Contracting Officer, through the COR or Personnel Security Specialist, within five (5) business days of contract award.
4. Low Risk Investigative Requirements
  - a. All investigations must be completed through the Electronic Questionnaires for Investigations Process (e-QIP). All contractors must complete the Authorization for Investigation Worksheet before they can complete the online e-Qip.
  - b. Optional Form 306, Declaration for Federal Employment provide by VA point of contact.

- c. Electronic Fingerprint Verification or FD 258, U.S. Department of Justice Fingerprint Applicant Chart.
- d. Once the items requested are completed, the Contractor is authorized to provide services under the contract. As previously stated, if the investigation or screening is not completed prior to the start date of the contract, the Contractor will be responsible for the actions of those individuals they provide to perform work for VA.
- e. The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the contract person from consideration of working under the contract.
- f. Failure to comply with these Contractor personnel security requirements may result in termination of the contract for default.

##### 5. Government Responsibilities

- a. The VA Contracting Officer will ensure a time for contract personnel to complete the fingerprint portion of this requirement, if any, and the COR will be responsible for performing any duties assigned by the VA Contracting Officer with regard to fulfilling the Contractor personnel security requirements described herein.
- b. Upon receipt, the local VA facility or VA SIC, depending on the type of investigation/screening required, will review the accuracy of the items requested in paragraph above, and forward these items to OPM to conduct their portion of the background investigation or screening, as applicable.
- c. The requesting VA facility will pay for any portion of the investigation or screening conducted by OPM, if any.
- d. Depending on the type of investigation/screening required, the Personnel Security Specialist, or VA SIC will notify the VA Contracting Officer of the adjudicating results of the background investigation or screening.
- e. The VA Contracting Officer and Personnel Security Specialist will ensure that the required investigations or screening have been completed or are in the process of being requested.

#### **Personnel Identity Verification (PIV) of Contractor Personnel**

In accordance with FAR 52.204-9 and VA Directive 0735 – Personal Identity Verification of Federal Employees and Contractors, any contract person who requires routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system will be required to verify their identity prior to providing services under the contract. Prior to providing services under the contract, each contract person will be asked to provide two (2) forms of identification from the Accepted Identification Documentation List to the appropriate VA representative in order to obtain a proper VA-issued identification card. See the Accepted Identification Documentation List provided below. The COR, or designee, will be responsible for sponsoring each contract person that requires a VA-issued identification card.

## PIV ID Proofing Criteria

The following criteria must be met by all VA employees, contractors, and affiliates prior to being issued a PIV card or Temporary Identity Badge.

### Table of Accepted Identification (From Form I-9)

Last Update: January 7, 2008

Picture ID From Federal or State Government	Non-Picture ID or Acceptable Picture ID not issued by Federal or State Government
<ul style="list-style-type: none"><li>• State-Issued Drivers License</li><li>• State DMV-Issued ID Card</li><li>• U.S. Passport</li><li>• Military ID Card</li><li>• Military Dependent's card</li><li>• US Coast Guard Merchant Mariner card</li><li>• Foreign Passport with appropriate stamps</li><li>• Permanent Resident Card or Alien Registration Card with a photograph (INS Form I-151 or I-551)</li><li>• ID Card issued by federal or state government agencies provided it includes a photograph.</li></ul>	<ul style="list-style-type: none"><li>• Social Security Card</li><li>• Certified Birth Certificate</li><li>• State Voter Registration Card</li><li>• Native American Tribal Document</li><li>• Certificate of U.S. Citizenship (INS Form N-560 or N-561)</li><li>• Certificate of Naturalization (INS Form N-550 or N-570)</li><li>• Certification of Birth Abroad Issued by the Department of State (Form FS-545 or Form DS-1350)</li><li>• Permanent or Temporary resident card.</li><li>• ID Card issued by local government agencies provided it includes a photograph or includes the following information: name, date of birth, gender, height, eye color, and address</li><li>• Non-photo ID Card issued by federal or state government agencies provided it includes the following information: name, date of birth, gender, height, eye color, and address</li><li>• School ID with photograph</li><li>• Canadian Drivers License</li><li>• US Citizen ID Card (Form I-179)</li></ul>

1. Two forms of identification are required from the above list of acceptable documents. Either of the following is accepted:
  - a. Two forms of identification from the left column (Federal or State Government issued picture ID)
  - b. One form of identification from the left column (Federal or State Government issued picture ID) and one form from the right column (Non-Picture ID or Acceptable Picture ID not issued by Federal or State Government).

2. The following rules apply for form identification:

- a. Any form of identification used for ID proofing may not be expired (except U.S. Passport)
- b. Department of Veterans Affairs site/facility badges are not accepted as a valid form of identification.
- c. VA PIV Cards are federally issued ID cards and can be used as a valid form of identification.
- d. Handwritten or photocopied documents are not accepted.
- e. An ID issued before a legal name change (e.g. birth certificate or driver's license) can be presented as one form of ID if a legal document (e.g. marriage certificate/license or a court order) is also presented linking the previous name to the current legal name. The linking document has to display both the former and current legal names. Both documents must be valid and not expired (except U.S. Passport). For example, a married woman may use both a certified copy of her birth certificate displaying her maiden name and a driver's license displaying her married name as the 2 forms of ID compliant with PIV Guidelines, as long as she provides a marriage license displaying both her maiden name and married name.
- f. The Applicant's name listed on the VA PIV Registration Portal, Request for One-VA Identification Card, must match the name on one of the IDs presented by the Applicant.
- g. The names on both forms of ID presented for ID proofing must match exactly. If one form of ID has a middle name or initial, the other form of ID must have a matching middle name or initial. One form can contain a middle name and the other can have a middle initial as long as they match. ALL names must be accounted for on both forms of ID. Please see the acceptable and unacceptable ID proofing examples provided below.

ACCEPTABLE NAME VARIATIONS

ID # 1 – John Henry Smith; ID # 2 – John Henry Smith

ID # 1 – John H. Smith; ID # 2 – John H. Smith

ID # 1 – John Henry Smith; ID # 2 – John H. Smith

UNACCEPTABLE NAME VARIATIONS

ID # 1 – John Henry Smith; ID # 2 – John Smith

ID # 1 – John H. Smith; ID # 2 – John Smith

### 3. Access to and Safeguard of VA Information/Computer Systems

- a. VA may provide contract personnel with access to VISTA and general files maintained on VA computer systems. Sharing of these access codes or misuse of VA information/computer systems is a Federal crime. When contract personnel no longer provide services to VA, the Contractor shall immediately inform the COR to deactivate their access. The COR is responsible for deactivation.
- b. Computer access will require VA Cyber Security Awareness Training annually and acknowledge all agreements prior to access. (See attachment for security requirements). The COR is responsible for ensuring and documenting this requirement.
- c. Contractor personnel with Computer access will take necessary precautions to safeguard information and prevent disclosures. If contract personnel suspect a compromised they will report such knowledge to the COR that same day.
- d. Remotely access will require prior approval from Information Security Officer (ISO).
- e. The Contractor shall make its internal policies and practices regarding the safeguarding medical electronic information available to VA. Contractors are not authorized to employ a lesser requirement than what is established by this document.
- f. Any changes in the VA directives during the term of this contract, shall be deemed to be incorporated into this contract.