

# **CONTRACTOR PERSONNEL BACKGROUND, SECURITY, AND TRAINING REQUIREMENTS**

## **BACKGROUND CHECK:**

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.

Reference:

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

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

1. Position Risk/Sensitivity – For all positions required under this contract, the position risk/sensitivity has been designated as: **Low Risk**

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**

2. 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.

3. 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.

#### **4. 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.

**5. 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 will be responsible for sponsoring each contract person that requires a VA-issued identification card.

### **SECURITY CLAUSE(S):**

#### **Section 1: GENERAL**

- a. Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.
- b. The contractor, their personnel, and their subcontractors shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and information system security as delineated in this contract.

#### **Section 2: ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS**

- a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.
- b. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be

in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. The contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor's employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

### **Section 3: VA INFORMATION CUSTODIAL LANGUAGE**

a. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

c. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

d. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

### **Section 4: SECURITY INCIDENT INVESTIGATION**

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees

shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

#### **Section 5: LIQUIDATED DAMAGES FOR DATA BREACH**

- a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.
- b. The contractor/subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.
- c. Each risk analysis shall address all relevant information concerning the data breach, including the following:
- (1) Nature of the event (loss, theft, unauthorized access);
  - (2) Description of the event, including:
    - (a) date of occurrence;
    - (b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
  - (3) Number of individuals affected or potentially affected;
  - (4) Names of individuals or groups affected or potentially affected;
  - (5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
  - (6) Amount of time the data has been out of VA control;
  - (7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
  - (8) Known misuses of data containing sensitive personal information, if any;
  - (9) Assessment of the potential harm to the affected individuals;
  - (10) Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and
  - (11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.
- d. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying monetary to the VA liquidated damages per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
- (1) Notification;
  - (2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
  - (3) Data breach analysis;
  - (4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

- (5) One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and
- (6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

#### **Section 6: CONTRACTOR REQUIRED TRAINING**

- a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
  - (1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix E relating to access to VA information and information systems;
  - (2) Successfully complete the VA Cyber Security Awareness and Rules of Behavior training and annually complete required security training;
  - (3) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
  - (4) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]
- b. The contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

#### **Section 7: SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES**

- a. The contractor, their personnel, and their subcontractors shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and information system security as delineated in this contract.

#### **Section 8: C&A**

- a. The C&A requirements do not apply and a Security Accreditation Package is not required.
- b. A Business Associate Agreement (BAA) is not required.

#### **CONTRACTOR QUALIFICATIONS AND TRAINING REQUIREMENTS:**

**Compliance and Business Integrity (CBI) Training:** CBI Awareness Training: The Contractor shall complete initial compliance awareness training within thirty (30) days of contract award effective date. The Contractor shall also meet the annual compliance awareness refresher training. This requirement can be fulfilled by completing the training module available via the following Internet site: <http://www.visn21.va.gov/CBI.asp>.