Attachment 1 – VA Information and Information System Security/Privacy

General

All contractors and contractor personnel shall be subject to the same Federal laws, regulations, standards and VA policies as VA, and VA personnel, regarding information and information system security. Contractors must follow policies and procedures outlined in VA Directive 6500, *Information Security Program* and its handbooks to ensure appropriate security controls are in place.

Access to VA Information and VA Information Systems

A contractor shall request logical (technical) and/or physical access to VA information and VA information systems for employees, subcontractors, and affiliates only to the extent necessary: (1) to perform the services specified in the contract, (2) to perform necessary maintenance functions for electronic storage or transmission media necessary for performance of the contract, and (3) for individuals who first satisfy the same conditions, requirements and restrictions that comparable VA employees must meet in order to have access to the same type of VA information.

All contractors and subcontractors working with VA Sensitive Information are subject to the same investigative requirements as those of regular VA appointees or employees who have access to the same types of information. The level of background security investigation will be in accordance with VA Directive 0710, Handbook 0710, which are available at: http://www1.va.gov/vapubs/ and VHA Directive 0710 and implementing Handbook 0710.01 which are available at: http://www.1.va.gov/vhapublications/index.cfm. Contractors are responsible for screening their employees. The following are VA's approved policy exceptions for meeting VA's background screenings/investigative requirements for certain types of contractors:

- Contract personnel not accessing VA information resources such as a personnel hired to maintain the medical facility grounds, construction contracts, utility system contractors, etc.,
- Contract personnel with limited and intermittent access to equipment connected to facility networks on which no VA sensitive information is available, including contractors who install, maintain, and repair networked building equipment such as fire alarm; heating, ventilation, and air conditioning equipment; elevator control systems, etc. If equipment to be repaired is located within sensitive areas (e.g. computer room/communications closets) VA IT staff must escort contractors while on site.
- Contract personnel with limited and intermittent access to equipment connected to facility networks on which limited VA sensitive information may reside, including medical equipment contractors who install, maintain, and repair networked medical equipment such as CT scanners, EKG systems, ICU monitoring, etc. In this case, Veterans Health Administration facilities must have a duly executed VA business

associate agreement (BAA) in place with the vendor in accordance with VHA Handbook 1600.01, Business Associates, to assure compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in addition to the contract. Contract personnel, if on site, should be escorted by VA IT staff.

The contractor agrees to –

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies.

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and,

(3) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of a system of records.

In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For the purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the contractor considered to be an employee of the agency.

(1) “Operation of a system of records” means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) “Record” means any item, collectin, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

(3) “System of records on individuals” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Security Incident Investigation

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 shall immediately notify the Contracting Officer Technical Representative (COTR) and simultaneously, the designated ISO/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 has access.

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

The contractor will simultaneously report the incident to the appropriate law enforcement entity(ies) of jurisdiction, including the VA Offices of the Inspector General and Security and Law Enforcement, in instances of theft or break-in or other criminal activity. The contractor, its employees, and its subcontractors and their employees will 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 will 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.

To the extent practicable, the contractor shall mitigate any harmful effects on individuals whose VA information was accessed or disclosed in a security incident. In the event of a data breach with respect to any VA Sensitive Information processed or maintained by the contractor or subcontractor under the contract, the contractor is responsible for liquidated damages to be paid to VA.

Security Controls Compliance Testing

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-day’s notice, at the request of the Government, the contractor will fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by VA in the event of a security incident or at any other time.

Training

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 networks:

(1) Sign and acknowledge understanding of and responsibilities for compliance with the attached National Rules of Behavior relating to access to VA information and information systems;

(2) Successfully complete VA Cyber Security Awareness training and annual refresher training as required;

(3) Successfully complete VA General Privacy training and annual refresher training as required; 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.]

The contractor shall provide to the contracting officer a copy of the training certificates for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required. These online courses are located at the following web site: https://www.ees-learning.net/.

Failure to complete this mandatory training within the timeframe required will be grounds for suspension or termination of all physical and/or electronic access privileges and removal from work on the contract until such time as the training is completed.

CONTRACTOR PERSONNEL SECURITY REQUIREMENTS:

a. All Contractor employees who require access to the Department of Veterans Affairs' computer systems shall be the subject of a background investigation and must receive a favorable adjudication from the VA Office of Security and Law Enforcement prior to contract performance. This requirement is applicable to all subcontractor personnel requiring the same access. If the investigation 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 the work for VA.

(1) Position Sensitivity – The position sensitivity has been designated as LOW RISK

2) Background Investigation – The level of background investigation commensurate with the required level of access is National Agency Check with Written Inquiries

(3) Cost of each Background Investigation **$254.00**

b. Contractor Responsibilities:

(1) The contractor shall bear the expense of obtaining background investigations. If the investigation is conducted by the Office of Personnel Management (OPM), the contractor shall reimburse VA within 30 days from receipt of a bill of collection. Background investigations from investigating agencies other than OPM are permitted if the agencies

possess an OPM and Defense Security Service certification. A Cage Code number must be provided to the Office of Security and Law Enforcement, which will verify the information and advise the contracting officer whether access to the computer systems can be authorized.

(2) The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain a U.S. citizenship, or are otherwise lawfully admitted to, and working in the United States, and are able to read, write, speak and understand the English language.

(3) After award and prior to contract performance, contractor will submit to the contracting officer:

(a) List of names of contractor personnel

(b) Social Security Numbers of contractor personnel

(c) Dates of birth of contractor personnel

(d) Contractor personnel email addresses

(e) Contractor personnel places of birth

(4) Contractor shall notify the Contracting Officer prior to changing/adding new contract personnel by submitting the above information.

(5) The Contractor shall submit or have Contractor employees submit the following required forms to the VA Office of Security and Law Enforcement within 30 days of receipt:

(a) Standard Form 85P, Questionnaire for Public Trust Positions

(b) Standard Form 85P-S, Supplemental Questionnaire for Selected Positions

(c) FD 258, U.S. Department of Justice Fingerprint Applicant Chart

(d) VA Form 0710, Authority for Release of Information Form

(e) Optional Form 306, Declaration for Federal Employment

(f) Optional Form 612, Optional Application for Federal Employment

(6) The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the contract.

(7) Failure to comply with the contractor personnel security requirements may result in termination of the contract for cause.

c. Government Responsibilities:

(1) The VA Office of Security and Law Enforcement will provide the necessary forms to the Contractor or to the Contractor's employee(s) after receiving a list of names and addresses.

(2) Upon receipt, the VA Office of Security and Law Enforcement will review the completed forms for accuracy and forward the forms to OPM to conduct the background investigation.

(3) The VA Office of Security and Law Enforcement will notify the contracting officer and contractor after adjudicating the results of the background investigations received from OPM.

(4) The Contracting Officer will ensure that the Contractor provides evidence that investigations have been completed or are in the process of being requested.