Department of Veterans Affairs
Office of Information & Technology

VA Information and Information System Security/Privacy Requirements for IT Contracts

Prepared by:

The Office of the Assistant Deputy Director for Information Protection and Risk Management (IPRM)

August 2008

VA Information and Information System Security/Privacy Requirements for IT Contracts

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://www1.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 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.

Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry safeguards the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. Defense Security Service (DSS) administers the NISP on behalf of the Department of Defense and 23 other federal agencies within the Executive Branch. VA will verify clearance through DSS.

VA Information Custodial Requirements

Information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor 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 contracting officer. This clause expressly limits the contractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d)(1).

Information generated by a Contractor as a part of the contractor's normal business operations, such as medical records created in the course of providing treatment, is subject to a review by the Office of General Counsel (OGC) to determine if the information is the property of VA and subject to VA policy. If the information is determined by OGC to not be the property of VA, the restrictions required for VA information will not apply.

VA information will not be co-mingled with any other data on the contractors/subcontractors information systems/media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. VA also reserves the right to conduct IT resource inspections to ensure data separation and on-site inspection of information destruction/media sanitization procedures to ensure they are in compliance with VA policy requirements.

Prior to termination or completion of this contract, contractor will not destroy information received from VA or gathered or created by the contractor in the course of performing this contract without prior written approval by the VA contracting officer. Any data destruction done on behalf of VA by a contractor must be done in accordance with National Archives and Records Administration (NARA)

requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, and applicable VA Records Control Schedules.

The contractor will receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. Applicable Federal information security regulations include all Federal Information Processing Standards (FIPS) and Special Publications (SP) issued by the National Institute of Standards and Technology (NIST). If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies, including FIPS or SP, in this contract.

Contractors collecting, storing, or disseminating personal identifiable information (PII) or protected health information (PHI) data must conform to all pertinent regulations, laws, and VA directives related to privacy. Contractors must provide access for VA privacy reviews and assessments and provide appropriate documentation as directed.

The contractor shall not make copies of VA information except as necessary to perform the terms of the agreement or to preserve electronic information stored on contractor electronic storage media for restoration in case any electronic equipment or data used by the contractor needs to be restored to an operating state.

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 terminate the contract for default or terminate for cause under Federal Acquisition Regulation ("FAR") part 12.

If a VHA contract is terminated for cause, the associated business associate agreement (BAA) will also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01 Business Associates.

Contractor will store, transport or transmit VA sensitive information in an encrypted form, using a VA-approved encryption application that meets the requirements of NIST's FIPS 140-2 standard.

The contractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA directives are available on the VA directives Web site at http://www1.va.gov/vapubs/.

Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor will refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

Notwithstanding the provision above, the contractor shall not release medical quality assurance records protected by 38 U.S.C. 5705 or records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus protected under 38 U.S.C. 7332 under any circumstances, including in response to a court order, and shall immediately refer such court orders or other inquiries to the VA contracting officer for response.

The contractor will not use technologies banned in VA in meeting the requirements of the contract (e.g., Bluetooth enabled devices).

Information System Design and Development

Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA policies developed in accordance with Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, VA Information Security Program). During the development cycle a privacy impact assessment will be completed, provided to the COTR, and approved by the VA Privacy Service in accordance with Directive 6508, VA Privacy Impact Assessment and its associated Handbook 6508.1

The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37 and VA Handbook 6500.

The contractor will be required to design, develop, or operate a System of Records on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C.552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

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 such 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 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 is 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, collection, 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.

Information System Hosting, Operation, Maintenance or Use

For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. The contractor security control procedures must be identical, not equivalent, to those procedures used to secure VA systems. A privacy impact assessment (PIA) must also be provided to the COTR and approved by VA Privacy Service prior to operational approval. All external Internet connections involving VA information must be reviewed and approved by VA prior to implementation.

Adequate security controls for collecting, processing, transmitting, and storing of personally identifiable information, as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls need to be stated within the PIA and supported by a risk assessment. If these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

Outsourcing (contractor facility/contractor equipment/contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (C&A) of the contractor's systems in accordance with NIST Special Publication 800-37 and VA Handbook 6500 and a privacy impact assessment of the contractor's systems prior to operation of the systems. Government-owned (government facility/government equipment) contractor-operated systems, third party or business partner networks require a system interconnection agreement and a memorandum of understanding (MOU) which detail what data types will be shared, who will have access, and the appropriate level of security controls for all systems connected to VA networks.

The contractor must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the information security officer (ISO) for entry into VA's Plan of Action and Milestone (POA&M) management process. The contractor will use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor procedures will be subject to periodic, unannounced assessments by VA officials. The physical security aspects associated with contractor activities will also be subject to such assessments. As updates to the system occur, an updated PIA must be submitted to the VA Privacy Service through the COTR for approval.

All electronic storage media used on non-VA leased or owned IT equipment that is used to store, process, or access VA sensitive information must have all VA sensitive information removed, cleared, sanitized, or destroyed in accordance with VA policies and procedures upon: (1) completion or termination of the contract or (2) disposal or return of the IT equipment by the contractor or any person acting on behalf of the contractor, whichever is earlier.

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.