CONTRACT SECURITY

1. REASON FOR ISSUE: This Handbook establishes the procedures to implement security policy, and communicate responsibilities and departmental framework for the Department of Veterans Affairs (VA) contracts and acquisitions.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Handbook establishes VA's procedures, responsibilities, and processes for implementing security in appropriate contracts and acquisitions. This Handbook applies to all VA Administration and Staff Offices and pertains to VA sensitive information which is stored, generated, transmitted or exchanged by VA, a contractor, subcontractor or a third party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor or subcontractor's electronic information system(s) operating for or on the VA's behalf.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OI&T) (005).

4. RELATED DIRECTIVE: VA Directive 6500, *Information Security Program.*

5. RESCISSIONS: None.

CERTIFIED BY:

/S/
Roger W. Baker
Assistant Secretary for Information
and Technology

BY DIRECTION OF THE SECRETARY VETERANS AFFAIRS:

/S/
Roger W. Baker
Assistant Secretary for Information
and Technology

Distribution: Electronic Only.

CONTRACT SECURITY

CONTENTS

LIST OF APPENDICES

CONTRACT SECURITY

1. PURPOSE AND SCOPE

a. This handbook establishes the security requirements, procedures, responsibilities, and departmental framework for ensuring that security is included in appropriate Department of Veterans Affairs (VA) contracts and acquisitions.

b. This handbook applies to all VA contracts in which VA sensitive information is stored, generated, transmitted or exchanged by a VA contractor, subcontractor or third-party, or on behalf of any of these entities regardless of format and whether it resides on a VA or a non-VA system, for the contractor, subcontractor, or third party to perform their contractual obligations to VA for the acquisition of goods or services where they stand in lieu of VA and act on VA's behalf. Other agreements that involve disclosures of VA sensitive information (e.g., Business Associate Agreement (BAA), Data user Agreement (DUA), Data Transfer Agreement (DTA), Memorandum of Understanding (MOU), or sharing, executive, or computer matching agreements with another federal agency that is subject to FISMA) are outside the scope of this handbook and are not governed by these provisions.

2. BACKGROUND

a. The Federal Information Security Management Act (FISMA) (116 Stat. 2946, 2950) states that "each agency shall…provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." Information security is an important business process and must be considered in all phases of an acquisition and contract life cycle to ensure that VA's sensitive information and information technology assets are adequately protected. Failure to adequately address security in appropriate VA agreements or solicitations can jeopardize mission success and undermine public confidence. Contracting Officials (CO) together with Chief Information Officers (CIO), Information Security Officers (ISO), Privacy Officers (PO), and legal counsel provide a valuable service in the acquisition and contracting process to help identify and mitigate security issues in solicitations, contracts, task orders, and third party agreements that involve VA's sensitive information.

b. When relying on contractors, subcontractors, or third party servicers or associates, VA transfers operational responsibilities for performing one or more business functions (e.g., Information Technology (IT) services) to these partners. However, it still remains VA's responsibility to ensure the protection of these assets is addressed via compliance with applicable security regulations and policy on the part of these partners and contractors.

c. In order to comply with FISMA and other Federal legislation, VA has established its Information Security Program by issuing VA Directive 6500 and its accompanying handbooks to assist in complying with this program. To ensure security is included in appropriate VA acquisitions and contracts, the following appendices are being issued with this Handbook to assist the field:

(1) *Checklist for Information Security in the Initiation Phase of Acquisitions*, Appendix A.

(2) *VA Acquisition Regulation (VAAR) Solicitation Provision and Contract Clause*, Appendix B.

(3) *VA Information and Information System Security/Privacy Language for Inclusion into Contracts, as Appropriate*, Appendix C.

(4) *Contractor Rules of Behavior*, Appendix D.

3. PROCEDURES

a. Information generated by a contractor or subcontractor as part of the contractor/subcontractor's normal business operations, such as health record information created in the course of providing treatment or health care services to VA's Veterans is subject to review to determine if the information is owned by VA and subject to VA security policy. VA sensitive information that has been properly disclosed by VA to the contractor is not subject to the VAAR security clause. If the information is not owned by VA, the requirements outlined in this Handbook do not apply and the VAAR security clause should not be added to the contract. The CO, the PO, and if required, Regional Counsel can be consulted. VA OIG counsel will conduct the review for the OIG generated contracts.

b. VA requires that facilities and program offices ensure that contractors, subcontractors, and third-party servicers or associates, or on behalf of any of these entities, regardless of format or whether the VA information resides on a VA system or contractor/subcontractor's electronic information system(s) operating for or on VA's behalf, employ adequate security controls as appropriate in accordance with VA directives and handbooks, regulations, guidance, and established service level agreements.

c. Information security requirements must be considered in all phases or stages of VA's procurement process. The applicable Program Manager, Information System Owner, and Information Owner are responsible for ensuring that the solicitation document includes the appropriate information security and privacy requirements. The information security requirements must be sufficiently detailed to enable service providers to understand what is required. A general statement that the service provider must agree to comply with applicable requirements is not acceptable. See Appendix C for a catalog of security and privacy language statements that have been developed, reviewed, and approved and can be used in contracts, as appropriate. This language summarizes for the contractors the most important Federal and VA policy issues that need to be addressed, as appropriate, in contracts to ensure adequate security and privacy controls are included in the contract vehicle. Additional security or privacy language can be added, as required. Program managers, project designers, and acquisition professionals must take security requirements, measures, and controls into account when designing and making agency acquisitions; appropriate security controls drive requirements, specifications, deliverables, and costs. Acquisition staffs need to consult information security officials to determine what level of security and which security controls may be required in this process. VA Handbook 6500, *Information Security Program*, provides the security requirements and policy for VA.

d. The applicable VA Program Manager, Information System Owner, Information Owner, the CO, PO, ISO, and the Contracting Officer's Technical Representative (COTR) are responsible for ensuring that VA information system security and privacy requirements, as appropriate, are implemented and complied with per the requirements detailed in the contract. Compliance and Records Management Officers should also be contacted, as appropriate, to ensure the requirements and language they require are included in the contract.

e. VA requires that all facilities and program offices monitor information security control compliance of their respective contracts and acquisitions by doing the following:

(1) Adhere to the security and privacy contract language as outlined in the contracts.

(2) Ensure that COs work with their COTR, ISO, and PO and other applicable staff to complete Appendix A for all service acquisitions and contracts. This appendix assists in determining the security requirements for VA acquisitions and contracts during the planning phase of the acquisition process. The checklist must be included as part of the overall contract file by the CO for new service acquisitions and contracts and a copy must be maintained in the applicable contracts file and accessible to the COTR, ISO, and PO.

(3) Ensure that contracting officials include VA's approved security clause, Appendix B, into any applicable contracts, if required as indicated by completing Appendix A. **NOTE**: The security clause in Appendix B is currently undergoing official VA rulemaking by the Office of Acquisitions and Logistics (OA&L). The final version of the clause may be revised after it is presented to the public for review via the *Federal Register*.

(4) Ensure that contractors, third party partners, and servicers implement the VA security and privacy requirements, as defined in the contract. These requirements can also be added to the contract Statement of Work (SOW). The requirements apply to applicable contracts in which VA sensitive information is stored, generated, transmitted, or exchanged by VA, a contractor, subcontractor or a third-party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor or subcontractor's electronic information system(s) operating for or on the VA's behalf.

(5) Ensure that contractor systems that have negotiated with VA to store, generate, transmit, or exchange VA sensitive information in a contractor developed and maintained system are certified and accredited (authorized), and registered and monitored in VA's Security Management and Reporting Tool (SMART) database that monitors FISMA compliance. The Program Manager and/or the ISO is responsible for contacting the Information Protection and Risk Management's (IPRM) Certification Program Office (CPO) within OI&T to register the system or to answer questions regarding the authorization of systems.

(6) Ensure that Certification and Accreditation (Authorization) (C&A), is accomplished in compliance with VA policy (per the results of the completed checklist provided in Appendix A) and VA Handbook 6500.3, *Certification and Accreditation of VA Information Systems*. The OI&T CPO within the Office of Cyber Security (OCS) must be contacted regarding procedures for C&A (Authorization) of contractor managed systems.

(7) Ensure that the Program Manager, the COTR and the CO, with the assistance of the ISO, monitor compliance with the contract or agreement security requirements throughout the

life of the contract. For IT systems, this includes ensuring that annual self-assessments are conducted by the contractor with appropriate Plan of Actions and Milestones (POA&M) initiated and completed.

(8) Ensure that service providers and contractors who have negotiated agreements with VA that involve VA sensitive information, but do not maintain systems that require C&A, complete a Contractor Security Control Assessment (CSCA) within 30 days of contract approval and annually on the due date of the contract renewal. The ISO/COTR or CO can also request that a CSCA be completed by the contractor anytime there are potential security issues identified or suspected by VA or to ensure that applicable security controls are being implemented. The completion of the CSCA by the contractor is the responsibility of the COTR. The CSCA template is maintained on the IPRM portal under the C&A Section. The COTR can contact the ISO to obtain a copy of the CSCA from the portal or to seek assistance in the completion of the assessment. The completed CSCA must be provided and reviewed by the ISO and by the CPO to ensure that adequate security is being addressed by contractors in situations where the C&A of a system is not applicable. A copy of the CSCA is uploaded by the ISO and maintained in the document section of the SMART database.

(9) Ensure that contractors and third party servicers accessing VA information sign the *Contractor Rules of Behavior*, Appendix D. The VA National Rules of Behavior do not need to be signed if the VA *Contractor Rules of Behavior"* are signed.

(10) Ensure that contractors and third party service positions receive the proper risk level designation based upon the review of the Position Designation System and Automated Tool (PDAT) established by the Operations, Security, and Preparedness Office (007). Background investigations of all contractors must adhere to the results of the PDAT per VA Directive and Handbook 0710, *Personnel Suitability and Security Program*.

(11) Ensure that contractors take the required security and privacy training as outlined in Appendix C.

(12) Ensure that all IT procurements, including contracts, are submitted through the IT Acquisition Request System (ITARS), VA's acquisition approval system for review and approval as required by the VA CIO.

(13) Ensure that language is included in appropriate contracts to ensure new acquisitions include Federal Desktop Core Configuration (FDCC) settings and products of information technology providers operate effectively using them.

4. RESPONSIBILITIES

a. **Secretary of Veterans Affairs** has designated the CIO as the senior Agency Official responsible for ensuring enforcement and compliance with the requirements imposed on VA under FISMA.

b. **Assistant Secretary for Office of Information and Technology (AS-OI&T)** is responsible for:

(1) Providing leadership for the Department-wide information security program;

(2) Approving all VA policies and procedures that are related to information security; and

(3) Authorizing a review process with assigned resources for the technical review of IT acquisitions, including contracts, to ensure that compliance with VA and Federal IT security standards and requirements are fulfilled per VA Directive and Handbook 6500.

c. **Assistant Secretary for Operations, Security, and Preparedness (AS-OSP)** has the authority to establish and maintain personnel security and suitability programs throughout the Department consistent with applicable laws, rules, regulations, and Executive Orders. The responsibilities include:

(1) Providing broad departmental-wide direction, standards setting, coordination, and performance assessment for organization components within VA and develop policies, procedures, and practices relating to background investigations of employees and contractors and the determinations of risk and sensitivity levels of employee position descriptions.

(2) Implementing appropriate laws, rules, and regulations related to the personnel security and suitability program and taking actions to address and correct conditions that are non-compliant with applicable laws, rules, and regulations.

d. **Associate Deputy Assistant Secretary for Acquisition and Logistics Programs and Policy** is responsible for:

(1) Providing acquisition policy to VA COs, Program Managers (PM) and COTRs to facilitate implementation of VA's information security program within the Department. This applies to all contracts in which VA sensitive information is stored, generated, transmitted, or exchanged by VA;

(2) Ensuring policy requires that the approved VAAR security clause is included in all applicable contracts; and

(3) Ensuring policy requires the CO consult with the COTR and the ISO, as necessary to monitor contracts to ensure that all Federal and VA security and privacy requirements are being met per the contract.

e. **Office of Inspector General (OIG)** is responsible for conducting regular reviews of the security program to ensure that all Federal and VA security and privacy requirements are being met.

f. **Office of General Counsel (OGC)** is responsible for providing guidance to the field regarding the applicability of the provisions in this handbook to specific VA contracts and agreements, as requested.

g. **Deputy Assistant Secretary for Information Protection and Risk Management** has been designated by the VA CIO, under the provisions of FISMA, to be the VA Chief Information Security Officer (CISO) and responsible for establishing, managing, and directing the VA Information Security and Risk Management Program. These responsibilities include:

(1) Establishing, maintaining, and monitoring Department-wide information security policies, procedures, control techniques, training, and auditing requirements as elements of the Department's Information Security Program; and

(2) Ordering and enforcing Department-wide compliance with and execution of any information security policy.

h. **Associate Deputy Assistant Secretary for Cyber Security** has been designated as the Deputy Chief Information Security Officer and is responsible for:

(1) Developing directives and handbooks to provide direction for implementing elements of the Information Security Program to all Department organizations; and

(2) Reviewing all policies and procedures related to information security under the management and oversight of other Department organizations.

i. **Associate Deputy Assistant Secretary for Risk Management and Incident Response** is responsible for providing incident response related to information security breaches throughout the Department.

j. **Associate Deputy Assistant Secretary for Privacy and Records Management** is responsible for:

(1) Providing guidance and procedures for protecting personally identifiable information (PII) as required by the Privacy Act of 1974;

(2) Providing oversight and guidance in order to ensure VA compliance with applicable privacy laws, regulations, and policies;

(3) Establishing VA requirements and providing guidance regarding the development, completion, and updating of Privacy Impact Assessments (PIA); and

(4) Ensuring that Privacy Awareness Training is provided and available for VA employees, contractors, volunteers, and interns.

k. **Under Secretaries, Assistant Secretaries, and Other Key Officials** are responsible for:

(1) Implementing the policies, procedures, practices, and other countermeasures identified in the Department's Information Security Program that comprise activities that are under their day-to-day operational control or supervision;

(2) Coordinating with OI&T and the CPO to periodically test and evaluate information security controls that comprise activities that are under their day-to-day operational control or supervision to ensure effective implementation; and

(3) Developing mechanisms for communicating, on an ongoing basis, each workforce member's roles and responsibilities specific to information security and privacy policies and practices to enhance VA's security and privacy culture.

l. **Program Directors and Facility Directors, through the ISO,** are responsible for:

(1) Ensuring compliant implementation and providing the necessary support to the Information Security Program in their organizations to ensure the facility meets all applicable information security requirements mandated by VA policy and other Federal legislation (e.g., FISMA, Health Insurance Portability and Accountability Act (HIPAA); and

(2) Ensuring ISOs are fully involved in all new projects concerning the development or acquisition of systems, equipment, or services including risk analysis, security plans, Request for Proposals (RFPs), and other procurement documents that require the ISO's participation.

m. **ISOs** are the agency officials assigned responsibility to ensure compliance with Federal security legislation and VA security directives and handbooks. The VA ISOs are responsible for:

(1) Supporting the Program Manager or Information System Owner during the requirements analysis phase by evaluating requirements and providing advice on appropriate security measures;

(2) Reviewing proposed SOWs to ensure that the resulting contracts and service providers sufficiently define information security responsibilities, provide a means to respond to information security problems, and include a right to terminate the contract if it can be shown that the contractor does not abide by the information security terms of the contract;

(3) Participating in the review and completion of Appendix A, *Checklist for Information Security in the Initiation Phase of Acquisitions*;

(4) Managing their local information security programs and serving as the principal security advisor to COTRs, COs, and PMs regarding security considerations in applications, systems, procurement or development, implementation, operation and maintenance, and disposal activities (e.g., life cycle management);

(5) Advising the PM or System Owners in coordinating the development and maintenance of information system security plans and contingency plans for contractor systems, as requested;

(6) Advising the PM or System Owners on the Certification and Accreditation (Authorization) process for applicable contractor systems;

(7) Assisting the COTR and CO in verifying and validating that appropriate security measures are implemented and functioning as intended in accordance with the contract or agreement provisions;

(8) Monitoring compliance with the security awareness and training requirements for each employee and contractor;

(9) Coordinating, monitoring, and conducting periodic reviews to ensure compliance with the Rules of Behavior requirement for each system information user;

(10) Serving as the primary point-of-contact for security awareness and training within their area of responsibility;

(11) Coordinating with the facility PO for the assurance of reasonable safeguards as required by VA policy, the HIPAA Privacy Rule as appropriate, and other Federal privacy statutes; and

(12) Consulting with the PO, as necessary, to monitor contracts to ensure that all Federal and VA privacy requirements are being met per the contract.

n. **Local Privacy Officers (PO)** are the agency officials assigned responsibility for managing the risks and business impacts of privacy laws and policies and they assist the ISO with the development and implementation of an information protection infrastructure for VA data. The VA POs assist by:

(1) Providing guidance for compliance with applicable privacy laws, regulations, and VA privacy policies, as required;

(2) Participating in the review and completion of Appendix A, *Checklist for Information Security in the Initiation Phase of Acquisitions*;

(3) Assisting PMs or Information System Owners and contractors in conducting PIAs, as required;

(4) Coordinating with and assisting ISOs with privacy-related issues in acquisition documents (i.e., SOWs, contracts, service agreements);

(5) Coordinating with COTRs and ISOs, as appropriate, to ensure that all privacy breaches involving VA sensitive information are reported to the VA-National Security Operations Center (VA-NSOC) within one hour of receipt of breach notification from the contractor;

(6) Coordinating with the appropriate facility officials, to restore or maintain compliance with the execution and administration of the BAA process, where applicable; and

(7) Monitoring the facility's BAAs to determine if the business associate meets the terms of their BAA with the facility.

o. **Program or Project Managers and Information Systems Owners who are requesting or managing a contract or service** must determine whether contractors or third party servicers require information access (documents or electronic) in the accomplishment of the VA mission. Specifically, these individuals are responsible for:

(1) Identifying information security and privacy requirements during the requirements analysis based on a specific analysis of availability, integrity, and confidentiality and the technical requirements of the contract;

(2) Participating in the review and completion of Appendix A, *Checklist for Information Security in the Initiation Phase of Acquisitions*;

(3) Ensuring appropriate security language is included in applicable contracts so that the Statement of Work (SOW) accurately reflects the requirements of the contract;

(4) Ensuring appropriate background investigations are initiated and verified on all contractors under their supervision through the VA Security and Investigations Center (SIC);

(5) Ensuring that all hardware and software purchases conform to VA's requirements;

(6) Ensuring that all system development efforts comply with the best practices, technical standards, and product standards of VA;

(7) Determining the contractor's "need to know" before access is granted. Access to any VA information or information system must not be authorized for a person who does not have a need for access to the system in the normal performance of that individual's official duties;

(8) Ensuring that periodic reviews of the project are conducted to ascertain whether information security has been maintained at the appropriate level and compliance with the information security program continued after award. All instances of noncompliance must be reported to the CO or designated representative, for necessary action;

(9) Ensuring users (including contractors) under their supervision or oversight complete all security and privacy training requirements;

(10) Ensuring users (including contractors) under their supervision or oversight review and sign the appropriate Rules of Behavior on an annual basis;

(11) Notifying system managers and ISO to revoke access privileges immediately when a user under their supervision or oversight (including contractors) no longer requires access privileges or fails to comply with this policy;

(12) Authorizing remote access privileges for contractors, if required, and reviewing remote access user security agreements on a regular basis to verify the continuing need for access and the appropriate level of privileges; and

(13) Conducting closeout activities, including the return of all VA sensitive information and information resources provided to the contractor during the life of the contract at the expiration or completion of the contract. See VA Handbook 6500, Appendix D.

p. **COs and COTRs** are responsible for:

(1) Supporting the PM and ISO during the requirements analysis phase by conducting market research and providing procurement planning assistance as needed, including

requirement specifics that address impact levels, security controls, and requirements in the acquisition, its plan, and its process;

(2) Participating in the review and completion of Appendix A, *Checklist for Information Security in the Initiation Phase of Acquisitions*;

(3) Reviewing incoming SOWs to ensure that information security has been addressed in the acquisition's requirements and deliverables and if not, coordinating with the requestor to ensure compliance with the VA Information Security Program;

(4) Ensuring that information security interests are represented and included as an evaluation factor during the evaluation period and as a performance measure during the life of the contract;

(5) Ensuring that the VAAR security clause and appropriate security language is included in contracts, if required;

(6) Ensuring that contractors sign the *Contractor Rules of Behavior* (Appendix D) on an annual basis;

(7) Maintaining the original or copy of the *Contractor Rules of Behavior* for the life of the contract;

(8) Ensuring contracts for services include appropriate background investigation requirements;

(9) Ensuring that the PDAT is used to appropriately designate in the Statement of Work or other written description of the assignment, the proper risk or sensitivity level for the contract employees;

(10) Ensuring that appropriate service providers and contractors who have negotiated agreements with VA, that involve VA sensitive information (but whose systems do not require C&A) complete an initial CSCA and one annually on the due date of their contract renewal;

(11) Ensuring that the CSCA is submitted to the ISO;

(12) Ensuring and documenting that contractors complete the required security and privacy awareness training initially and then annually thereafter;

(13) Ensuring that contractors know when and how to report security and privacy incidents;

(14) Monitoring the contract and the contractor to ensure that the contract's security and privacy requirements and responsibilities are being implemented; and

(15) In coordination with the facility PO, ensuring that contracts for services involving access to or disclosure of, protected health information have appropriate business associate agreements.

5. REFERENCES

a. *Federal Information Security Management Act of 2002*, Public Law 107-347§ 208, 116 Stat. 2946 (2002)

b. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 § 264, 110 Stat. 1936 (2003)

c. Privacy Act of 1974, 5 U.S.C. 552a

d. 15 U.S.C. §278g-3

e. 38 U.S.C. §5721-28

f. 40 U.S.C. §11331

g. 44 U.S.C. Chapter 35

h. OMB Circular A-130, Management of Federal Information Resources (November 28, 2000)

i. OMB M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)

j. OMB M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems (March 22, 2007)

k. OMB M-07-18, Ensuring New Acquisitions Include Common Security Configurations (June 1, 2007)

l. OMB Memorandum for Chief Information Officers/Chief Acquisition Officers, Reminder – Ensuring Competition When Acquiring Information Technology and Using Common Security Configurations (December 19, 2007)

m. OMB M-07-19, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 25, 2007)

n. OMB M-09-02, Information Technology Management Structure and Governance Framework (October 21, 2008)

o. OMB M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (August 20, 2009)

p. National Institute of Standards and Technology: Federal Information Processing Standards (FIPS) http://scrc.nist.gov/publications/fips/index.html

q. National Institute of Standards and Technology Special Publications 800 Series http://csrc.nist.gov/publications/nistpubs/index.html

r. Federal Acquisition Regulations, 48 C.F.R. Parts 39 and 52.

s. VAAR – 852.273-75 Security Requirements for Unclassified Information Technology Resources (Interim – October 2008)

t. VA Directive and Handbook 6500, *Information Security Program*

u. VA Directive 6502, *VA Enterprise Privacy Program*

v. VA Directive and Handbook 0710, *Personnel Suitability and Security Program*

w. VA Handbook 6500.1, *Electronic Media Sanitization*

x. VA Handbook 6500.2, *Management of Security and Privacy Incidents*

y. VA Handbook 6500.3, *Certification and Accreditation of VA Information Systems*

z. VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*

aa. VHA Handbook 1600.01, *Business Associate Agreements*

bb. VHA Handbook 1605.1, *Privacy and Release of Information*

6. DEFINITIONS

1. **Acquisition** - Acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

2. **Acquisition Planning -** The process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency need in a timely manner and at a reasonable cost. It includes developing the overall strategy for managing the acquisition, agency requirements, plans of action and milestones for the acquisition process and award.

3. **Business Associate** - A business associate is an entity, including an individual, company, or organization that, on behalf of the VHA facility, performs or assists in the performance of functions or activities involving the use of disclosure of protected health information (PHI), or that provides certain services involving the disclosure of PHI by VHA.

4. **Business Associate Agreement** - A contract between VHA and a business associate, entered into before releasing PHI to the business associate, in order for the business associate to perform a covered activity for VHA.

5. **Certification and Accreditation (Authorization) (C&A) -** The process used to ensure information systems including Major Applications (MA) and General Support Systems (GSS) have effective security safeguards which have been implemented, planned for, and documented in a system security plan as commensurate with potential risks to the system's information.

6. **Contract -** Contract means a mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; interagency agreements (Economy Act or otherwise); job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications. Contracts do not include grants and cooperative agreements covered by 31 U.S.C. 6301, et. seq.

7. **Contract Clause or "Clause"** - A term or condition used in contracts or in both solicitations and contracts, and applying after contract award or both before and after award.

8. **Contracting** - Purchasing, renting, leasing, or otherwise obtaining supplies or services from non-Federal sources. Contracting includes description (but not determination) of supplies and services required, selection and solicitation of sources, preparation and award of contracts, and all phases of contract administration. It does not include making grants or cooperative agreements.

9. **Contracting Officer -** Person with the authority to enter into, administer, and terminate contracts and make related determinations and findings. The term includes certain authorized representatives of the CO acting within the limits of their authority as delegated by the CO. "Administrative Contracting Officer (ACO)" refers to a CO who is administering contracts. "Termination Contracting Officer (TCO)" refers to a CO who is settling terminated contracts. A single contracting officer may be responsible for duties in any or all of these areas.

10. **Contracting Officer's Technical Representative (COTR) or Contracting Officer Representative (COR) -** Individual designated and authorized in writing by the CO to perform specific technical or administrative functions.

11. **Federal Desktop Core Configuration (FDCC) -** An OMB (U.S. Office of Management and Budget) mandate, requiring all Federal Agencies standardize the configuration of approximately 300 settings on each of their Windows XP and Vista Computer. The reason for this standardization is to strengthen Federal IT security by reducing opportunities for hackers to access and exploit government computer systems.

12. **Federal Information System -** An information system (44 U.S.C. 3502(8)) used or operated by a Federal agency, or a contractor or other organization on behalf of the agency.

13. **Federal Information Security Management Act** (**FISMA) -** FISMA was passed by Congress and signed into law by the President as part of the E-Government Act of 2002 (Public Law No. 107-347). The goals of FISMA include development of a comprehensive framework to protect government information, operations, and assets.

14. **Information Security** (defined by FISMA, section 3542(b)(1)(A-C) - Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (i) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (ii) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (iii) availability, which means ensuring timely and reliable access to and use of information.

15. **Information Security Officer (ISO) -** Individual responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.

16. **Information Technology -** Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

17. **Personal Services Contract -** A contract that, by its express terms or as administered, makes the contractor personnel appear to be, in effect, government employees.

18. **Privacy Impact Assessment (PIA) -** An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

19. **Privacy Officer -** Employee(s) designated to implement and monitor compliance with privacy related laws, regulations, and VA policies at the facility.

20. **Plan of Action and Milestones (POA&M) -** A plan used as a basis for the quarterly reporting requirements of the Office of Management and Budget that includes the following information: (i) a description of the security weakness; (ii) the identity of the office or organization responsible for resolving the weakness; (iii) an estimate of resources required to resolve the weakness by fiscal year; (iv) the scheduled completion date; (v) key milestones with estimated completion dates; (vi) any changes to the original key milestone date; (vii) the source that identified the weakness; and (viii) the status of efforts to correct the weakness. A POA&M may also be used as a guide to the acquisition planning and development process as well as a guide to establishing a schedule of deliverables and metrics.

21. **VA Contractor Rules of Behavior -** A set of Department rules that describes the responsibilities and expected behavior of personnel with regard to access to and use of VA information assets and resources.

22. **Security Program -** (defined by FISMA, Section 3544(b)(1-8) **-** Each agency shall develop, document, and implement an agency wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

23. **Security Requirements -** Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet laws, Executive Orders, directives, policies, or regulations.

24. **Sensitive Personal Information (SPI) -** SPI is any information about an individual that can reasonably be used to identify that individual that is maintained by VA, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, telephone number, driver's license number, credit card number, photograph, finger prints, biometric records, etc., including any other personal information
linked or linkable to an individual.

25. **SMART Database -** A database established by VA to maintain FISMA security requirements and the field's compliance with the requirements. It also contains the plan of actions and milestones required to meet the mandated requirements.

26. **System of Records Notice (SORN) -** A statement providing public notice of the existence and character of 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. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.

27. **VA Data or Information -** Information owned by VA and in the possession of VA or any entity acting for or on the behalf of VA.

28. **VA Sensitive Information -** All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or

deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

29. **Vendor -** Supplier of goods and services to other companies.

ACRONYM LIST

Abbreviation / Acronym	Description
ADAS	Associate Deputy Assistant Secretary
BAA	Business Associate Agreement
BI	Background Investigation
C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Contracting Officer
COR	Contracting Officer's Representative
COTR	Contracting Officer Technical Representative
FAR	Federal Acquisition Regulation
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
IPRM	Information Protection and Risk Management
ISO	Information Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NSOC	National Security Operations Center
OI&T	Office of Information and Technology
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
PDAT	Position Designation System and Automated Tool
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PO	Privacy Officer
POA&M	Plan of Action and Milestones
PWS	Performance Work Statement
RFI	Request for Information
RFP	Request for Proposals
SMART	Security Management and Reporting Tool
SOO	Statement of Objectives
SOW	Statement of Work
SPI	Sensitive Personal Information
VA	Department of Veterans Affairs
VAAR	VA Acquisition Regulation

CHECKLIST FOR INFORMATION SECURITY IN THE INITIATION PHASE OF ACQUISITIONS

1. BACKGROUND

In accordance with VA policy, contractors' storage, generation, transmission or exchanging of VA sensitive information requires approriate security controls to be in place. The VA Information Security Program policy – VA Directive and Handbook 6500 and additional 6500 series directives and handbooks - provide the framework for security within VA.

2. INSTRUCTIONS

This checklist must be completed at the **initiation** of all IT service acquisitions, statements of work, third-party service agreements and any other legally binding agreement in order to determine what, if any, security and privacy controls are necessary specifically as it relates to the VAAR security clause. OGC guidance should be sought on data ownership issues, as necessary. The checklist can also be used for other types of contracts, if appropriate or needed. In order to successfully complete this checklist, each question below must be addressed in coordination with all members of the local Acquisition Team including: the Procurement Requestor or Program Manager from the program office or facility, the Contracting Officer Representative (COR), the Information Security Officer (ISO), the Contracting Officer (CO) from the program office or facility's servicing Acquisition office, and the Privacy Officer (PO). The ISO is the arbitrator if there are questions or disagreements on the appropriate answers.

1.	Does the contract involve "VA sensitive information?" (See 3. PROCEDURES a.) If yes, proceed to next question. If no, then the security clause is not required.	Yes ☐ No ☐
2.	Is this an acquisition or purchase of only commodities or goods (e.g. equipment or software)? If yes, then the security clause is not required as long as VA sensitive information is not involved. If no, then proceed to the next question.	Yes ☐ No ☐
3.	Will this acquisition require services of contractor personnel? If no, proceed to question 5. If yes, proceed to next question.	Yes ☐ No ☐
4.	Will the personnel perform a function that requires access to a VA system or VA sensitive information (e.g., system administrator privileged access to a VA system, or contractor systems or processes that utilize VA sensitive information)? NOTE: See 3.a. under PROCEDURES regarding contracts and agreements concerning medical treatment for Veterans. If the answer above is no, then proceed to the next question. If yes, then VA security policies apply. Contracting Officials need to work with the Program Manager or (procurement requestor), COTR, PO, and ISO to: i. Include the appropriate risk designation of the contractors based on the PDAT determination. ii. Incorporate the security clause (Appendix B) into the contract involved and the appropriate security/privacy language outlined in Appendix C into the solicitation. iii. Determine if protected health information is disclosed or accessed and if a BAA is required.	Yes ☐ No ☐

5.	Will this acquisition require use of a contractor-owned Information Technology (IT) system or computer assets, **and**	Yes ☐ No ☐
	a. The IT system hardware components are located at an offsite contractor facility; **and**	Yes ☐ No ☐
	b. The IT system is **not** connected to a VA network; and	Yes ☐ No ☐
	c. The contractor has exclusive administrative control to the components; **and**	Yes ☐ No ☐
	d. The purpose of the requirement for the system is to process or store VA information on behalf of the VA.	Yes ☐ No ☐
	If <u>any</u> of the answers to 5a-5d are <u>no</u>, proceed to the next question. If <u>yes</u>, then VA security policies apply. Incorporate the clause from Appendix B and the appropriate security/privacy language from Appendix C respectively into the solicitation and contract and initiate planning for the certification and accreditation of the contractor system(s). Contracting Officials need to work with the COTR and ISO to: • Determine the security impact of the IT system as High, Moderate, or Low per 6500 Handbook, *Information Security Program*. • Ensure Contractor understanding of the IT security requirements for certification and accreditation (authorization) (C&A) of the contractor system. See VA Handbook 6500.3, *Certification and Accreditation*. • Ensure that the proper VA Management Official is appointed by the Certification Program Office to formally authorize operation of the system in accordance with VA Handbook 6500 and 6500.3. • Enforce contractor performance (timely submission of deliverables, compliance with personnel screening requirements, maintenance of secure system configurations and participation in annual IT Federal Information Security Management Act (FISMA) assessments to ensure compliance with FISMA requirements). • Ensure yearly FISMA assessments are completed and uploaded into SMART.	

6.	Will this acquisition require services that involve connection of one or more contractor-owned IT devices (such as a laptop computer or remote connection from a contractor system) to a VA internal trusted (i.e., non-public) network? If no, then include a statement in the SOW that "The C&A requirements do not apply, and that a Security Accreditation Package is not required: and proceed to the next question. If yes, then incorporate the security clause from Appendix B and the appropriate security/privacy language from Appendix C respectively into the solicitation and contract. Contracting Officials need to work with the COR and the ISO to: • Ensure contractor understands and implements the IT security requirements for system interconnection documents required per the Memorandum of Understanding or Interconnection Agreement (MOU-ISA). The standard operating procedure (SOP) and a template for a MOU-ISA are located on the Information Protection Risk Management (IPRM) Portal and can be provided to the contractor. • Ensure contractor understands their participation in IT security requirements for C&A of the VA system to which they connect. • Enforce contractor performance (timely submission of deliverables, compliance with personnel screening requirements, and appropriate termination activity as appropriate).	Yes ☐ No ☐
7.	Is the acquisition a service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a MOU-ISA for system interconnection? If no, then specify the mechanism/documentation used to ensure the VA sensitive information is protected. If yes, then incorporate the security clause and the appropriate security language from Appendices B and C into the solicitation and contract. The COTR needs to: • Ensure that a Contractor Security Control Assessment (CSCA) is completed within 30 days of contract approval and yearly on the renewal date of the contract.	Yes ☐ No ☐

	• Ensure that the CSCA is sent to the ISO and the OCS Certification Program Office for review to ensure that appropriate security controls are being implemented in service contracts. • Ensure a copy of the CSCA is maintained in the Security Management and Reporting Tool (SMART) database. COTR will provide a copy of the completed CSCA to ISO for uploading into SMART database.	

3. SIGNATURES

Please provide the name and telephone number of each Acquisition Team member who participated in completing this checklist. By signing this checklist, the Contracting Officer is representing that Security was considered for this requirement through coordination with members of the Acquisition Team including the program or requesting office's IT Security point of contact.

(1) **Contracting Officer Representative**:

Name:	Phone:
Signature:	Date:

(2) **Information Security Officer**:

Name:	Phone:
Signature:	Date:

(3) **Contracting Officer:**

Name:	Phone:
Signature:	Date:

(4) **ProcurementRequestor/Program Manager:**

Name:	Phone:
Title:	
Signature:	Date:

(5) **Privacy Officer:**

Name:	Phone:
Signature:	Date:

(6) **Other Team Members participating in the acquisition (e.g., Records Management Officer/Compliance Officer):**

Name:	Phone:
Title:	
Signature:	Date:

VA ACQUISITION REGULATION SOLICITATION PROVISION AND CONTRACT CLAUSE

NOTE: This clause will undergo official rule making by the Office of Acquisitions and Logistics. The below language will be submitted for public review through the *Federal Register*. The final wording of the clause may be changed from what is outlined below based on public review and comment. Once approved, the final language in the clause can be obtained from the Office of Acquisitions and Logistics Programs and Policy.

1. SUBPART 839.2 – INFORMATION AND INFORMATION TECHNOLOGY SECURITY REQUIREMENTS

839.201 Contract clause for Information and Information Technology Security:

a. Due to the threat of data breach, compromise or loss of information that resides on either VA-owned or contractor-owned systems, and to comply with Federal laws and regulations, VA has developed an Information and Information Technology Security clause to be used when VA sensitive information is accessed, used, stored, generated, transmitted, or exchanged by and between VA and a contractor, subcontractor or a third party in any format (e.g., paper, microfiche, electronic or magnetic portable media).

b. In solicitations and contracts where VA Sensitive Information or Information Technology will be accessed or utilized, the CO shall insert the clause found at 852.273-75, Security Requirements for Unclassified Information Technology Resources.

2. 852.273-75 - SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (INTERIM- OCTOBER 2008)

As prescribed in 839.201, insert the following clause:

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.

(END OF CLAUSE)

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE

1. GENERAL

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.

2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A contractor/subcontrator 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. 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 contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. 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.

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. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor 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*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d. The contractor/subcontractor must 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. 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 or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

e. 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.

f. 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.

g. 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.

h. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

i. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor 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/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.

4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, 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 (PIA) must be completed, provided to the COTR, and approved by the VA Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.

b. The contractor/subcontractor shall certify to the COTR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

c. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.

d. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

e. 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, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

f. The contractor/subcontractor is required to design, develop, or operate a System of Records Notice (SOR) 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.

g. The contractor/subcontractor 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:

(a) The Systems of Records (SOR); and

(b) The design, development, or operation work that the contractor/subcontractor 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 SOR on individuals that is subject to the Privacy 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 SOR.

h. 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 SOR 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 SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the contractor/subcontractor 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 SOR, including the collection, use, maintenance, 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 identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

(3) "System of Records" 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.

i. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

j. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than ____ days.

k. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within ____ days.

l. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerablity scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be 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 to VA's network involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), 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 are to be assessed and stated within the PIA and 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.

c. Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The contractor/subcontractor's system 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 ISO for entry into VA's POA&M management process. The contractor/subcontractor must 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/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may

affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The contractor/subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COTR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or contractor/subcontractor-owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the contractor/subcontractor or any person acting on behalf of the contractor/subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

(1) Vendor must accept the system without the drive;

(2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

(3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

(4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

(a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

(b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the purchase order or contract.

(c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

6. 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 COTR 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.

7. 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 to the VA liquidated damages in the amount of $_____ 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.

8. 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 must 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) as determined by VA in the event of a security incident or at any other time.

9. 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.

CONTRACTOR RULES OF BEHAVIOR

This User Agreement contains rights and authorizations regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the Department of Veterans Affairs (VA). This User Agreement covers my access to all VA data whether electronic or hard copy ("Data"), VA information systems and resources ("Systems"), and VA sites ("Sites"). This User Agreement incorporates Rules of Behavior for using VA, and other information systems and resources under the contract.

1. GENERAL TERMS AND CONDITIONS FOR ALL ACTIONS AND ACTIVITIES UNDER THE CONTRACT:

a. I understand and agree that I have no reasonable expectation of privacy in accessing or using any VA, or other Federal Government information systems.

b. I consent to reviews and actions by the Office of Information & Technology (OI&T) staff designated and authorized by the VA Chief Information Officer (CIO) and to the VA OIG regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA. These actions may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing to all authorized OI&T, VA, and law enforcement personnel as directed by the VA CIO without my prior consent or notification.

c. I consent to reviews and actions by authorized VA systems administrators and Information Security Officers solely for protection of the VA infrastructure, including, but not limited to monitoring, recording, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized OI&T, VA, and law enforcement personnel.

d. I understand and accept that unauthorized attempts or acts to access, upload, change, or delete information on Federal Government systems; modify Federal government systems; deny access to Federal government systems; accrue resources for unauthorized use on Federal government systems; or otherwise misuse Federal government systems or resources are prohibited.

e. I understand that such unauthorized attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. This includes penalties for violations of Federal laws including, but not limited to, 18 U.S.C. §1030 (fraud and related activity in connection with computers) and 18 U.S.C. §2701 (unlawful access to stored communications).

f. I agree that OI&T staff, in the course of obtaining access to information or systems on my behalf for performance under the contract, may provide information about me including, but not limited to, appropriate unique personal identifiers such as date of birth and social security number to other system administrators, Information Security Officers (ISOs), or other authorized staff without further notifying me or obtaining additional written or verbal permission from me.

g. I understand I must comply with VA's security and data privacy directives and handbooks. I understand that copies of those directives and handbooks can be obtained from the Contracting Officer's Technical Representative (COTR). If the contractor believes the policies and guidance provided by the COTR is a material unilateral change to the contract, the contractor must elevate such concerns to the Contracting Officer for resolution.

h. I will report suspected or identified information security/privacy incidents to the COTR and to the local ISO or Privacy Officer as appropriate.

2. GENERAL RULES OF BEHAVIOR

a. Rules of Behavior are part of a comprehensive program to provide complete information security. These rules establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the information it contains is an essential part of their job.

b. **The following rules apply to all VA contractors.** I agree to:

(1) Follow established procedures for requesting, accessing, and closing user accounts and access. I will not request or obtain access beyond what is normally granted to users or by what is outlined in the contract.

(2) Use only systems, software, databases, and data which I am authorized to use, including any copyright restrictions.

(3) I will not use other equipment (OE) (non-contractor owned) for the storage, transfer, or processing of VA sensitive information without a VA CIO approved waiver, unless it has been reviewed and approved by local management and is included in the language of the contract. If authorized to use OE IT equipment, I must ensure that the system meets all applicable 6500 Handbook requirements for OE.

(4) Not use my position of trust and access rights to exploit system controls or access information for any reason other than in the performance of the contract.

(5) Not attempt to override or disable security, technical, or management controls unless expressly permitted to do so as an explicit requirement under the contract or at the direction of the COTR or ISO. If I am allowed or required to have a local administrator account on a government-owned computer, that local administrative account does not

confer me unrestricted access or use, nor the authority to bypass security or other controls except as expressly permitted by the VA CIO or CIO's designee.

(6) Contractors' use of systems, information, or sites is strictly limited to fulfill the terms of the contract. I understand no personal use is authorized. I will only use other Federal government information systems as expressly authorized by the terms of those systems. I accept that the restrictions under ethics regulations and criminal law still apply.

(7) Grant access to systems and information only to those who have an official need to know.

(8) Protect passwords from access by other individuals.

(9) Create and change passwords in accordance with VA Handbook 6500 on systems and any devices protecting VA information as well as the rules of behavior and security settings for the particular system in question.

(10) Protect information and systems from unauthorized disclosure, use, modification, or destruction. I will only use encryption that is FIPS 140-2 validated to safeguard VA sensitive information, both safeguarding VA sensitive information in storage and in transit regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA.

(11) Follow VA Handbook 6500.1, *Electronic Media Sanitization* to protect VA information. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR's orders.

(12) Ensure that the COTR has previously approved VA information for public dissemination, including e-mail communications outside of the VA as appropriate. I will not make any unauthorized disclosure of any VA sensitive information through the use of any means of communication including but not limited to e-mail, instant messaging, online chat, and web bulletin boards or logs.

(13) Not host, set up, administer, or run an Internet server related to my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA unless explicitly authorized under the contract or in writing by the COTR.

(14) Protect government property from theft, destruction, or misuse. I will follow VA directives and handbooks on handling Federal government IT equipment, information, and systems. I will not take VA sensitive information from the workplace without authorization from the COTR.

(15) Only use anti-virus software, antispyware, and firewall/intrusion detection software authorized by VA. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR's orders regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with VA.

(16) Not disable or degrade the standard anti-virus software, antispyware, and/or firewall/intrusion detection software on the computer I use to access and use information assets or resources associated with my performance of services under the contract terms with VA. I will report anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages to the COTR.

(17) Understand that restoration of service of any VA system is a concern of all users of the system.

(18) Complete required information security and privacy training, and complete required training for the particular systems to which I require access.

3. ADDITIONAL CONDITIONS FOR USE OF NON- VA INFORMATION TECHNOLOGY RESOURCES

a. When required to complete work under the contract, I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA approved remote access software and services.

b. Remote access to non-public VA information technology resources is prohibited from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.

c. I will not have both a VA network line and any kind of non-VA network line including a wireless network card, modem with phone line, or other network device physically connected to my computer at the same time, unless the dual connection is explicitly authorized by the COTR.

d. I understand that I may not obviate or evade my responsibility to adhere to VA security requirements by subcontracting any work under any given contract or agreement with VA, and that any subcontractor(s) I engage shall likewise be bound by the same security requirements and penalties for violating the same.

4. STATEMENT ON LITIGATION

This User Agreement does not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

5. ACKNOWLEDGEMENT AND ACCEPTANCE

I acknowledge receipt of this User Agreement. I understand and accept all terms and conditions of this User Agreement, and I will comply with the terms and conditions of this agreement and any additional VA warning banners, directives, handbooks, notices, or directions regarding access to or use of information systems or information. The terms and conditions of this document do not supersede the terms and conditions of the signatory's employer and VA.

Print or type your full name	Signature
Last 4 digits of SSN	Date
Office Phone	Position Title
Contractor's Company Name	**Please complete and return the <u>original</u> signed document to the COTR within the timeframe stated in the terms of the contract.**