A. GENERAL INFORMATION

1. Title of Project: Gastroenterology Clinical Documentation System

2. Scope of Work: The contractor shall provide all resources necessary to accomplish the deliverables described in this statement of work (SOW), except as may otherwise be specified. Contractor shall provide Gastroenterology Clinical Documentation System meeting minimum specifications contained herein. Work shall meet all applicable codes and regulations, drawings, and is subject to the terms and conditions of the contract.

3. Background: The Atlanta Veterans Affairs Medical Center is purchasing a clinical documentation system specific to gastroenterological procedures to replace an obsolete and tedious methodology currently being used. The system will streamline workflows thereby increasing procedure throughput, standardize procedure documentation increasing accuracy and completeness for improved patient care, and provide a searchable database for trending and retrieval of patient data. The system shall also include endoscopy image management for capture and storage of still and video images from existing Olympus endoscopy equipment. The system shall provide preoperative and postoperative as well as intraoperative procedure documentation. In addition, the system will provide processes to assist with financial aspects for recovery of costs through the insurance billing process through existing VA management systems.

4. Performance Period: The contractor shall complete the work required under this SOW in 60 calendar days or less from date of award, unless otherwise directed by the Contracting Officer (CO). If the contractor proposes an earlier completion date, and the Government accepts the contractor's proposal, the contractor's proposed completion date shall prevail. Work at the Government site shall not take place on Federal holidays or weekends unless directed by the CO.

5. Type of Contract: Firm-Fixed-price.

B. CONTRACT AWARD MEETING

The contractor shall not commence performance on the tasks in this SOW until the CO has conducted a kick off meeting, or has advised the contractor that a kick off meeting is waived.

C. GENERAL REQUIREMENTS

For every task, the contractor shall identify in writing all necessary subtasks (if any), associated costs by task, and along with associated sub-milestone dates. The contractor's subtask structure shall be reflected in the technical proposal and detailed work plan.

All written deliverables shall be phrased in layperson language. Statistical and other technical terminology shall not be used without providing a glossary of terms.

Where a written milestone deliverable is required in draft form, the VA will complete their review of the draft deliverable within 7 calendar days from the date of receipt. The contractor shall have 60 calendar days to deliver the final deliverable from date of receipt of the Government's comments.

D. SPECIFIC MANDATORY TASKS AND ASSOCIATED DELIVERABLES

Description of Tasks and Associated Deliverables: The contractor shall provide the specific deliverables described below within the performance period stated in Section A.4 of this SOW.

Task One: Deliver a commercially available, off-the-shelf clinical documentation system for gastroenterology procedures comprised of software and related hardware in a turn-key fashion that meets all technical requirements contained herein.

Delivery of the Gastroenterology clinical documentation system shall be planned, scheduled, and coordinated with the Atlanta VAMC Logistics, Biomedical Engineering, and Gastroenterology Departments. Installation and implementation shall occur with the least disruption to patient care.

Installation of hardware and software as well as any networking components shall be the responsibility of the contractor with coordination through Biomedical Engineering.

Configure software and hardware for the gastroenterology clinical documentation system.

Deliverable One: Verification of proper and functional installation of a Gastroenterology clinical documentation system in specified locations within the Gastroenterology Department or other data center location.

Task Two: Provide training for clinical users

Deliverable Two: Verification of training for clinical users as specified in agreement.

Task Three: Provide full service literature, preferably in electronic format, including technical manual, to VAMC Atlanta Biomedical Engineering.

Deliverable Three: Verification of receipt of full service literature, preferably in electronic format, including technical manual.

Task Four: Provide a minimum of two VAMC Biomedical Engineering Support Specialists technical training to include theory, function, repair, system administration, and maintenance of the installed Gastroenterology clinical documentation system.

Deliverable Four: Completion of training for 2 Biomedical Equipment Support Specialists.

Task Five: Provide complete software support including all application support for up to 4 optional years in addition to the first year of warranty. This is a subscription service required for continued operation of system.

Deliverable Five: Verify documentation of available subscription options to occur after first year warranty.

E. SALIENT CHARACTERISTICS

The following are the salient characteristics for the replacement patient beds at specified locations in the Atlanta VAMC.

1. GI clinical procedure documentation must be able to report and track the following procedures and events, minimum:
    a. Capsule endoscopy
    b. Colonoscopy
    c. Enteroscopy
    d. Endoscopic retrograde cholangiopancreatography (ERCP)
    e. Colonoscopy
    f. Flexible sigmoidoscopy
    g. Liver Biopsy
    h. Upper endoscopic ultrasound (EUS)
    i. pH studies and manometry
    j. Upper Endoscopy
    k. Preoperative processes
    l. Postoperative processes
    m. Procedure type counts by the enterprise and facility locations
    n. Scheduling for patients, physician, and supporting staff
    o. Patient cancellations, no-show and reschedule
    p. Procedure time, patient check-in to procedure time, to discharge time
    q. Patient recall and follow-up care

2. Server and workstation hardware shall be supplied by the contractor and meet the following requirements:
    a. Servers shall be rack mountable to meet technical requirements for software application and interfacing.
    b. Operating systems for servers and workstations shall be the latest supported software available, e.g. Microsoft Server 2016, Windows 10.
    c. Contractor shall complete a VA Directive 6550 Pre-Procurement for

Medical Device/Systems.

d. Provide a certificate for FIPS 140-2 compliance.
e. Power requirements not to exceed 110V 20A.
f. Redundant hard disk system to provide fail over capability.
g. Redundant power supplies or redundant servers.
h. Workstations shall be small form factor and meet the technical requirements for the software application and interfacing.

3. System shall provide a searchable data base which will allow a single or multiple variable data base search. Searches shall be allowed on all parameters configured within the patient record data base.

4. System shall provide for a unified procedure note in which nursing pre-procedural, intra-procedural, and post-procedural notes may be linked to the physician's notes to provide a single patient procedure record. Scanning of notes and "cut & paste" techniques are not allowed.

5. Allow images, still or video, to be captured directly from the procedure workstations using HD SDI, other HD video sources, and/or composite video sources during the procedure and placed in the procedural record. Capture and store still or video images is primarily from Olympus endoscopy imaging systems into the patient chart. System shall be capable of comparing and annotating images into patient chart.

6. Provide generation of specimen labels which are linked to the procedure record. Specimen label information and format shall be consistent with current and user-modifiable to VA Clinical Laboratory requirements.

7. System shall provide a bi-directional HL7 interface with the VA VistA system such that consult orders are sent or queried from VistA and the image and text results are transmitted back to VistA/CPRS. This will be accomplished through the VistA Clinical Procedures system. Interface must be single sign-on such that physician does not have to sign in to multiple systems to complete reports.

8. System shall provide CPT and ICD10 procedure coding for billing with capability of interfacing to VA Financial Systems for insurance cost recovery. System must be capable of updating codes as they may change.

9. System shall provide a method of intuitive navigation through the procedure documentation process. Content should be procedure specific.

10. System shall provide for standard report templates and unlimited custom report templates with e-signature capability.

11. System shall provide custom templates for printing of letters to referring physicians, post-procedure instruction, discharge instruction, and so forth.

12. System shall have capability to customize workflow interface to fit the current Gastroenterology workflow processes with ability to adjust for future needs.

13. System shall provide for pre-procedure and post-procedure documentation.

14. System shall provide interfacing to Philips MX450 patient monitor for acquisition of patient vital signs.

15. System shall have the ability to track endoscope processing history, e.g. scope usage from patient, room, physician, and nurse.

16. System shall provide quality assurance data such as GIQuIC registry, bowel preparation quality, adenoma detection rate, colonoscopy withdrawal time, colonoscopy depth of insertion, patient no-show rate, and so forth.

17. System shall provide real time patient tracking from admission to discharge via large screen displays strategically placed in the Gastroenterology procedure area.

18. Contractor shall provide user training for physicians, nurses, and technicians on how to use the system and software safely and effectively. Number of hours to be determined.

19. Contractor shall provide for annual clinical refresher training or when there are significant changes in the software.

20. Contractor shall provide technical training that covers maintenance and software administration as well as continued updates of the software and hardware that may be required.

21. Provide a minimum 5 years of software subscription services.

F. DESCRIPTION

The Contractor shall deliver, install, configure and implement a perioperative and postoperative gastroenterology documentation information system in accordance with specifications contained herein to the Atlanta VAMC, 1670 Clairmont Road, Atlanta, GA 30033. The system shall interface with the Clinical Procedures, Computerized Patient Record System (CPRS), and the VA Vista Imaging system. The Contractor shall also interface the system with the existing Philips Monitoring System in use at the Atlanta VAMC Endoscopy unit to encompass vital signs data into the information system.

The system shall include:

1. Medical gastroenterology preoperative, intraoperative, and postoperative documentation software and database
2. Server hardware required for system operation
3. Data reporting
4. Ability to customize forms
5. Clinically intuitive navigation for the documentation process
6. Integration with ICD 10 codes
7. Six (6) intraoperative capture workstations and associated documentation software
8. Two (2) travel cart intraoperative capture workstations and associated documentation software
9. Twenty (20) preoperative/postoperative documentation workstations including associated software
10. Eight (8) staff documentation workstations including associated software
11. Three (3) MD staff documentation workstations (w/large display) including associated software
12. Two (3) MD documentation workstations (w/70-inch display) for patent tracking
13. HL7 Result (ORU)/ PDF export interface to CPRS and PACS (VistA Imaging) via Clinical Procedures
14. HL7 Orders Interface via Clinical Procedures
15. Six (6) color network laser printers
16. Eight (8) label printers for specimen tracking
17. Five (5) years of software subscription support

G. CHANGES TO STATEMENT OF WORK

Any changes to this SOW shall be authorized and approved only through written correspondence from the CO. A copy of each change will be kept in a project folder along with

all other products of the project. Costs incurred by the contractor through the actions of parties other than the CO shall be borne by the contractor.

H. CONFIDENTIALITY AND NONDISCLOSURE

It is agreed that:

1. The preliminary and final deliverables, and all associated working papers, application source code, and other material deemed relevant by VA which have been generated by the contractor in the performance of this task order, are the exclusive property of the U.S. Government and shall be submitted to the CO at the conclusion of the task order.

2. The CO will be the sole authorized official to release, verbally or in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this task order. No information shall be released by the contractor. Any request for information relating to this task order, presented to the contractor, shall be submitted to the CO for response.

3. Press releases, marketing material, or any other printed or electronic documentation related to this project, shall not be publicized without the written approval of the CO.

I. CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

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

1. Position Sensitivity – The position sensitivity has been designated as (Insert High Risk, Moderate Risk or Low) Risk.

2. Background Investigation – The level of background investigation commensurate with the required level of access is _____.

3. Contractor Responsibilities

   a. The contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain a U.S. citizenship, and are able to read, write, speak and understand the English language.

   b. The contractor shall submit or have their employees submit the required forms (SF 86 or SF 85P, SF 85P-S, FD 258, Contractor Fingerprint Chart, VA Form 0710, Authority for Release of Information Form, and Optional Forms 306 and 612) to the VA Office of Security and Law Enforcement within 30 days of receipt.

   c. The contractor, when notified of an unfavorable determination by the Government, shall withdraw the affected employee from working under the contract.

d. Failure to comply with contractor personnel security requirements may result in termination of the contract for default.

4. Government Responsibilities

a. The VA Office of Security and Law Enforcement will provide the necessary forms to the contractor, or to the contractor's employees, after receiving a list of names and addresses.

b. Upon receipt, the VA Office of Security and Law Enforcement will review completed forms for accuracy and forward the forms to the office of Personnel Management (OPM) to conduct background investigations.

c. The VA Office of Security and Law Enforcement will notify the CO, and contractor, of adjudication results received from OMB.

J. INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY

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.
As determined by VA Privacy or Information Security, the contractor shall be required to enter into and sign a Business Associate Agreement upon award of contract unless a national BAA exists.

Access to Information and Information Systems

1. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

2. 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.

3. 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.

4. 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.

5. 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.

Information Custody

1. 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).

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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 COR.

Information System Hosting, Operation, Maintenance, or Use

1. 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 vulnerability 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 COR 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.

2. 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.

3. 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.

4. 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.

5. 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 COR. 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.

6. 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.

7. 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.

8. 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.

Security Incident Investigation

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

2. 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.

3. 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.

4. 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.

5. 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 $__37.50____ per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

    a. Notification;

    b. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

    c. Data breach analysis;

    d. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

    e. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

    f. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

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-days' 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.

Training

1. 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:

2. 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:

    a. Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;

    b. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

    c. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access.

3. The contractor shall provide to the contracting officer and/or the COR 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.

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 completed.

K. 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.

General Terms And Conditions for All Actions And Activities Under the Contract

1. Understand and agree that there is no reasonable expectation of privacy in accessing or using any VA, or other Federal Government information systems.

2. 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 access to and use of any information assets or resources associated with the 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 prior consent or notification.

3. 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.

4. 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.

5. 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).

6. Agree that OI&T staff, in the course of obtaining access to information or systems on the contractor's behalf for performance under the contract, may provide information about contractor personnel 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.

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

8. Contractor will report suspected or identified information security/privacy incidents to the COR and to the local ISO or Privacy Officer as appropriate.

General Rules of Behavior

1. 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.

2. The following rules apply to all VA contractors:

a. 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.

b. Use only systems, software, databases, and data which they are authorized to use, including any copyright

c. Contractor 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.

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