

**Statement Of Work**  
NAA/PCR Viral ID & Gene Mutation Instrument  
Southeast Louisiana Veterans Health Care System  
New Orleans, LA

08/22/2016

**1. PURPOSE**

- 1.1 The overall purpose is to provide and install NAA/PCR Viral ID & Gene Mutation Instruments for the Pathology & Laboratory Medicine Service at the Southeast Louisiana Veterans Health Care System (SLVHCS) 2400 Canal St, via 2401 Tulane Ave Whse, New Orleans, LA 70119.

**2. SCOPE**

- 2.1 The Contractor shall provide, transport, install, and test all listed equipment. All products must meet all salient characteristics defined in this section.
- 2.2 All equipment and installation must meet manufacturers and VA specifications.
- 2.3 The Contractor shall furnish all supplies, equipment, facilities and services required for delivery and installation of the supplies and equipment.
- 2.4 The Contractor is responsible for any missing parts and components not included in order to carry out the installation.

**2.5 SALIENT CHARACTERISTICS**

**2.5.1 NAA/PCR Viral ID & Gene Mutation Instrument**

Equivalent to Roche COBAS 4800 System

- Shall perform multi-channel pipetting, extraction, purification, nucleic acid target preparation and real-time PCR amplification and detection
- Shall perform HPV, HSV 1 & 2, KRAS, BRAF, EGFR, and LDTs testing.
- Fully automated and software driven with ready-to-use bar-coded, room temperature reagents
- Must have an air displacement system which eliminates the need for large batches of wash buffer, system priming, and the disposal of large volumes of liquid waste
- System's software shall allow the end user individual choice of reporting schema per sample within any batch for HPT tests.
- System shall have a HPV test with HPV high risk pool plus HPV 16 & 18 genotype simultaneously (HR12+1+1+1) , as well as a traditional high risk pool (14 HR genotypes)
- For HSV 1 and 2 testing the system shall use unique primer pairs and probes for the detection of 5 targets: DNA polymerase region B and thymidine Kinase region C for the detection of HSV1, glycoprotein B 3' end region and thymidine kinase C for the detection of HSV 2 and an internal control
- Performs fully automated sample preparation from primary vials
- All PCR reactions shall contain AmpErase enzyme in the Master Mix for contamination control from previously generated amplicon
- System shall prevent cross contamination by securely locking pipette tips in place to avoid motions that could create aerosols of samples and reagents
- Performs real-time PC using optical channels which detects multiple targets from one reaction tube
- The instrument shall have a total aspirate and dispense monitoring system to ensure valid results by monitoring the pressure within tips to detect low volumes and clogs with pressure response that fall outside the expected range are reported as errors.

- Must use ready-to-use, load and go reagents with no thawing or mixing required
- Performs real-time PCR with digital data capture provides accurate qualitative results with no gray zone which eliminates the need for equivocal sample retesting
- Must use an advanced results algorithm eliminates the need for manual curve analysis
- The instrument shall analyze each test automatically with a kinetic algorithm so results are clearly positive, negative or invalid
- The system shall accommodate multiple sample types and flexible batch sizes with easy to use software interface
- The system shall use automatic internal controls to minimize the potential for false negative results
- The instrument shall have one year warranty on parts and labor
- The instrument shall be FDA approved
- The vendor shall supply all materials needed to validate the instrument
- The instrument must be able to transmit results through an HL7 interface using Data Innovations Instrument Manager Middleware

2.5.2 Data Innovations Instrument Manager Interface connection to primary server to include license and connection box.

2.5.3 Data Innovations Instrument Manager Interface connection to backup server to include license and connection box.

2.5.4 Installation of instrument with assurance of proper operation shall be provided by the manufacturer.

2.5.5 One Year Warranty must include all parts and labor and preventative maintenance on the instrument at no cost to the Government for the period of 4/28/2017 to 4/27/2018.

2.5.6 Necessary reagents, test kits, supplies, and clinical specimens for validation and correlation studies on instrument at no cost to the Government

- Vendor must work with COR to determine parameters of validations study
- For validation and correlation studies, expiration dating period of the consumables shall not be less than six (6) months at the time of delivery to the facility

2.5.7 On-site training at no costs for two (2) key operators and VA technical staff on instrumentation and software

2.5.8 Off- site training at no cost for two (2) key operators on instrumentation and software

2.5.9 On-site or Off-site training for two (2) Biomedical Engineers on instrumentation (includes airfare, transportation, lodging and meals), if available.

2.5.10 Extended warranty for 1 year past the initial warranty, where service and preventative maintenance is Included for the period of 4/27/2018 to 4/28/2019.

## 2.6 DELIVERY AND INSTALLATION

### 2.6.1 DELIVERY

- 2.6.1.1 Contractor shall deliver all equipment to the Pathology & Laboratory Medicine Service, Room 4F122B at the Southeast Louisiana Veterans Health Care System (SLVHCS) 2400 Canal St, New Orleans, LA 70119 on 4/21/2017 via the 2401 Tulane Avenue, New Orleans, LA 70119 loading dock.
- 2.6.1.2 Deliver materials to job in manufacturer's original sealed containers with brand name marked thereon.
- 2.6.1.3 Package to prevent damage or deterioration during shipment, handling, storage and installation. Maintain protective covering in place and in good repair until removal is necessary.
- 2.6.1.4 Deliver specified items only when the site is ready for installation work to proceed.
- 2.6.1.5 Store products in dry condition inside enclosed facilities.
- 2.6.1.6 Any government requested delayed delivery up to 90 days after initial delivery date, shall be at no additional cost to the Government.
- 2.6.1.7 A pre-delivery meeting will be conducted 60 days prior to initial negotiated delivery date for verification of delivery and installation dates.
- 2.6.1.8 Delivery and Installation will be coordinated through the COR

## 2.6.2 INSTALLATION

- 2.6.2.1 Install all equipment to manufacturer's specifications maintaining Federal, and Local safety standards
- 2.6.2.2 Installation must be completed by 4/28/2017. All work shall be completed between 8:00 a.m. and 4:30 p.m. Monday – Friday. All federal holidays, excluded. Federal holidays are available at the [Federal Holiday OPM Site](#).
- 2.6.2.3 If there is an operational conflict with installation, night or weekend installation may be required. Government will provide a 72 hours' notice of change of installation hours.
- 2.6.2.4 The contractor shall coordinate all deliveries, staging areas, installations, and parking arrangements with the COR.
- 2.6.2.5 The Contractor shall remove all related shipping debris and cleanup any construction associated with delivery and installation of the specified items. Contractor shall remove all packaging from the SLVHCS premises. The Contractor shall be responsible for any damage to the building that occurs due to Contractor error or neglect.

## 2.7 SITE CONDITIONS

- 2.7.1 There shall be no smoking, eating, or drinking inside the hospital at any time.

## 3. INSPECTION AND ACCEPTANCE:

- 3.1 The Contractor shall conduct a joint inspection with the VA COR upon delivery of equipment.
- 3.2 Contractor shall provide dates of completion of punch list items and replacement parts and/or short ship items from the manufacturer(s).
- 3.3 The COR shall ensure all work is completed satisfactorily prior to acceptance. Disputes shall be resolved by the Contracting Officer.

## 4. DELIVERABLES

- 4.1 Operation and Maintenance Manuals
  - 4.1.1 Binders - Quantity (2) each for items 3.1 - 3.17
  - 4.1.2 Digital Copies in CD Form- Quantity (1) each for items 3.1 – 3.17
- 4.2 Deliver compilation of all manufacturer recommended maintenance schedule and operation materials packaged in binder(s) to COR upon completion of installation.

## 5. OPERATOR TRAINING

- 5.1 Contractor shall provide Vendor led, on-site, instrument training. This training shall include two (2) Key Operators and all of the VA Technical staff on the operation of the hardware and software systems; data manipulation; basic troubleshooting and repair; instrument validation and method comparison studies; as well as basic troubleshooting and repair.
- 5.2 The contractor shall ensure two (2) VA key operators (Technical Staff) are fully trained and competent to operate

and troubleshoot the system.

- 5.3 Contractor shall install, test, train VA employees, and complete all quality assessment of the analyzer by 5/5/2017. All work shall be completed between 8:00 a.m. and 4:30 p.m. Monday-Friday; all Federal holidays, excluded. Federal holidays are available at the [Federal Holiday OPM Site](#).
- 5.4 The Contractor shall provide off-site training on the instrument for two (2) VA key operators; the cost must include travel, lodging, meals, transportation and training if available.
- 5.5 Contractor shall coordinate training so that it is timely to the equipment installation, be consistent with the size and scope of the facility's services and be minimally equivalent to that offered in the commercial marketplace. The contractor will provide annual training for at least two VA operators per year or according to established FSS contract if applicable.
- 5.6 Contractor shall schedule training or changes in training dates with the COR

## 6. PROTECTION OF PROPERTY

- 6.1 Contractor shall protect all items from damage. The Contractor shall take precaution against damage to the building(s), grounds and furnishings. The Contractor shall repair or replace any items related to building(s) or grounds damaged accidentally or on purpose due to actions by the Contractor.
- 6.2 The Contractor shall perform an inspection of the building(s) and grounds with the COR prior to commencing work. To insure that the Contractor shall be able to repair or replace any items, components, building(s) or grounds damaged due to negligence and/or actions taken by the Contractor. The source of all repairs beyond simple surface cleaning is the facility construction contractor (or appropriate subcontractor), so that building warranty is maintained. Concurrence from the VA Facilities Management POC and COR is required before the Contractor may perform any significant repair work. In all cases, repairs shall utilize materials of the same quality, size, texture, grade, and color to match adjacent existing work.
- 6.3 The Contractor shall be responsible for security of the areas in which the work is being performed prior to completion.
- 6.4 Contractor shall provide floor protection while working in all VA facilities. All material handling equipment shall have rubber wheels.

## 7. SECURITY REQUIREMENTS

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

b. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. 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.

## **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.

## **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.

d. VA training site is located at [www.tms.va.gov](http://www.tms.va.gov)

There is only one course the contractor needs to complete and print the certificate at the end. A copy of the completed certificate must be submitted before work begins (within 5 business days of contract award).

+++++

**Instructions to get to the Courses in TMS**

[www.tms.va.gov](http://www.tms.va.gov)

Log onto the site and create a new user account; if you already don't have one. Search for your course entitled [VA Privacy and Information Security Awareness and Rules of Behavior](#). Complete course, print certificate (s), and sign/print contractor rules of behavior.

VA Learning University (VALU)

**Help Desk: 1-866-496-0463**

[valmshelp@va.gov](mailto:valmshelp@va.gov)

+++++

**Examples**



## [VA Privacy and Information Security Awareness and Rules of Behavior](#)



### **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.

## **10. 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 the 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.

a. The CO will be the sole authorized official to release verbally or in writing, any data, the draft deliverables, the 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.

b. 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.

## **8. WARRANTY**

8.1 The contractor shall provide a one year manufacturer's warranty on all parts and labor.

8.2 The warranty shall include all travel and shipping costs associated with any warranty repair.