

STATEMENT OF WORK
FOR
STERIS STEAM STERILIZERS

1. **GENERAL:** Provide service, parts, labor, and transportation to perform preventive maintenance, calibration and repair on the following Steris systems used at the Bay Pines VA Healthcare System.
2. **SCOPE OF WORK:** The contractor shall provide all supplies, materials, parts, equipment, labor, tools, Software, supervision, management and transportation to perform all tasks identified below, for Steris equipment at the C.W. Bill Young VAMC. All equipment, listed below, shall be maintained in proper operating condition as specified by the manufacturer. Contractor is to have proven access to original equipment manufacturers parts, manuals and schematics, which shall be available on site to perform the service

The following equipment is located at C.W. Bill Young VA Medical Center 10000 Bay Pines Blvd, Bay Pines, Florida 33744:

EE#37745 SN: 011030425 Steris (Century V-116) Sterilizer Rm# 2D-151-100
EE#37747 SN: 010910403 Steris (Century V-116) Sterilizer Rm# 2D151-100
EE#45198 SN: 3630605001 Steris (Reliance 130L) Cart Washer Rm# 1C108-100
EE#77398 SN: 0311C1184 Steris (CAVI-20W-E) Ultrasonic Cleaner Rm# 1C102-100

- a. **UPGRADES:** Hardware and software upgrades shall be scheduled and performed during normal working hours at no additional charge to the VA. Upgrades shall be those required for the correct function of the system; not those purchased to enhance function. The above designated equipment may change with technological advances and the agreement requires flexibility to modify equipment requirements.
- b. **CALIBRATIONS:** Calibrations shall be completed at the manufacturer's recommended frequency; using certified test equipment. The contractor's field service engineers shall respond by phone within 2 hours and on site within 48 hours to complete repairs. Uptime requirements, excluding scheduled preventive maintenance, will be 97% of the normal working hours and working days during the term of the contract. All broken parts removed to repair the system, will become the property of the contractor, with the exception of material containing electronic protected healthcare information. The contractor is responsible for the disposal of these parts.
- c. **WORK HOURS:** Hours of coverage will be from 8:00am – 8:00pm EST, Monday through Friday, excluding Federal Holidays (New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day,

Veterans Day, Thanksgiving Day, and Christmas Day). All work done outside the normal coverage time should be first approved by the Contracting Officer's Representative (COR). Preventive maintenance shall be negotiated, during normal hours, at least one month in advance with the COR. Preventive maintenance will be done at the manufacturer's recommended frequency.

- d. PARTS AND MATERIALS: The contractor will provide all service manuals, and will not have access to manuals purchased by the VA. Parts and upgrades shall be manufacture approved and compatible with the equipment being maintained. The contractor shall have adequate spare parts inventory available 24/7 for immediate or emergency repairs or upgrades.
- e. REPORTS: Each scheduled and unscheduled visit shall result in the production of a written report, by the contractor's technician, in a format negotiated between the COR and the contractor. The contractor shall contact the COR before and after arrival at the site.
- f. TECHNICIANS: Personnel performing maintenance and repair shall be fully qualified, competent Field Service Engineers (FSE). "Fully Qualified" is based upon training and on experience in the field. The COR reserves the right to reject any of the contractor's personnel and refuse them permission to work on the VAMC equipment; if deemed necessary. The contractor shall provide a 24/7 emergency telephone number for repair service.

3. VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

VA INFORMATION CUSTODIAL LANGUAGE:

- a. 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.
- b. 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.
- c. 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.

d. 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.

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 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.

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.

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.

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:

a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete VA Privacy and Information Security Awareness and Rules of Behavior Training 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 *Rules of Behavior* before being granted access to VA information and its systems.

b. The contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the 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.

NOTE: The Certification and Accreditation (C&A) requirements do not apply and a Security Accreditation Package is not required for this SOW.