Pharmacy Cleanroom Viable Sampling and Fingertip Testing

Introduction:

The VAMC West Palm Beach is seeking to establish a firm fixed price contract for one base year period and two option year periods at the discretion of the Government. The estimated totals by category are provided under the requirements section.

General Information

Semi Annual Pharmacy Viable Surface and Air Microbiologic Testing for ISO/USP regulated sterile compounding areas and equipment within the Department of Pharmacy for all Hazardous and Non-hazardous compound medications and Annual Fingertip Testing.

Scope of Work: The contractor shall provide monthly inspection and testing, including viable

surface and air microbiologic testing in all ISO-classified areas, including all West Palm Beach Pharmacy Hoods, Clean Rooms, Anterooms, and Pass-Throughs in accordance with the most current CETA Certification Application Guide on USP 797 Viable Environmental Sampling and

Gowning Evaluation. The contractor shall provide semi-annual viable surface and air microbial

testing to include mold and yeast utilizing Malt Extract Agar (MEA) and bacteria using

Trypticase Soy Agar (TSA). If CFU levels measured during viable sampling exceed USP797

threshold levels, the report will at minimum identify genus and, when possible, species of any

microorganism recovered on the monthly report, in addition to the location of the CFU and

specific recommendations for remediation. The contractor will deliver the results of sampling in

detail by sample location, CFU count, genus, and when possible, species in a report which

addresses recommendations for remediation on all positive results.

Background: VA West Palm Beach seeks a USP 797 Clean Room CETA-Certified contractor for improving VA West Palm Beach Pharmacy Services compliance with USP 797 requirements **and to provide a second layer of oversight over internal processes.**

Performance Period: The contract term is for Base Plus (4) Years.

Hours of work: Work required in the performance of the contract shall be performed during

hours agreed upon between the Contractor and TVHS Pharmacy Supervisors.

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.

GENERAL REQUIREMENTS:

USP<797> requires each person which performs compounding to pass this test. The person tested will aseptically place their fingertips into petri dishes containing tryptic soy agar. Must occur once every twelve months for low/medium risk compounding.

**This testing will be done annually and the first testing will be completed within 30 days of the contract award date. This testing may be requested of new personnel as hired throughout the year.**

Gloved Fingertip Sampling Approx. 24-30 $\_\_\_\_ per person total $\_\_\_\_\_\_\_

**CONTACT PLATE SAMPLING**

USP<797> requires each controlled area to be sampled at “locations of risk” for viable organisms on surfaces. Utilizing the two-plate method, flat surfaces in risk areas are sampled utilizing an adversarial method on tryptic soy agar and sabouraud dextrose plates. Testing must occur at least semi-annually. **This testing will be completed semi-annually. The first testing will be completed within 30 days of the contract award date. The second testing will be done 6 months after completion of the first test. For Option Years to ensure continuity of periodic testing all samplings will be performed within 30 days of the dates that correspond to when the previous year testing was completed. This testing must be completed at the same time as the Active air sampling.**

Contact Plate-Room 64 $\_\_\_\_ each plate total $\_\_\_\_

Contact Plate-Device 7 $\_\_\_\_ each plate total $\_\_\_\_

**SURFACE SWAB SAMPLING**

USP<797> requires each controlled area to be sampled at “locations of risk” for viable organisms on surfaces. Utilizing a swab, irregular surfaces in risk areas are sampled utilizing an adversarial method on tryptic soy broth. Testing must occur at least semi-annually. IDENTIFICATION OF GROWTHS. **This testing will be completed semi-annually and the first testing will be completed within 30 days of the contract award date. The second testing will be done 6 months after completion of the first test. For Option Years to ensure continuity of periodic testing all samplings will be performed within 30 days of the dates that correspond to when the previous year testing was completed.**

**This testing will be completed at the same time as the Active air sampling.**

Swab Test 39 $\_\_\_\_ per location total $\_\_\_\_\_

USP<797> requires each colony forming unit, (growths) to be identified, whether the number of cfu’s is actionable or not. Following the appropriate incubation any plates or swabs indicating growth are sent to an accredited microbiology lab for identification to the genus level. **This testing will be completed semi-annually and the first testing will be completed within 30 days of the contract award date. The second testing will be done 6 months after completion of the first test. For Option Years to ensure continuity of periodic testing all samplings will be performed within 30 days of the dates that correspond to when the previous year testing was completed. This testing will be completed at the same time as the Active air sampling.**

Growth Identification 142 $\_\_\_\_ per plate total $\_\_\_\_

Failure to comply with the packaging and/or marking requirements indicated herein, or incorporated herein by reference, may result in rejection of the merchandise and request for replacement or repackaging, repacking, and/or marking. The Government reserves the right, without obtaining authority from the Contractor, to perform the required repackaging, repacking, and/or marking services and charge the contractor at the actual cost to the Government for the same or have the required repackaging, repacking, and/or marking services performed commercially under Government order and charge the Contractor at the invoice rate.

In connection with any discount offered, time will be computed from the date of completion of such repackaging, repacking and/or marking service.

The contractor will submit written report of date, location and genus of any detected colony

forming units (CFU) from the sampling, and when possible, the contractor will also report the

species of any microorganism recovered on the monthly report, as well as specific

recommendations for remediation. If no CFU s are detected, that will also be reported. This

report of sampling results will be submitted no later than 15 business days after the contractor receives the sampling results.

2. Sampling shall be scheduled with the COR and a West Palm Beach Pharmacy Supervisor a minimum of three (3) working days in advance. Close coordination with the COR and Pharmacy

Supervisor is necessary. Contractor will be responsible for ensuring all samplings are

completed semi-annually for all Pharmacy Cleanrooms at West Palm Beach. Fingertips will be completed annually and intermittently during the year should the need arise. Department of Pharmacy will communicate with the contractor any questions arising from the report within one week of receipt. No communication will be considered acceptance of the

report.

3. Any work requiring decontamination of contractor Equipment/Components shall be performed per manufacturer instructions and guidelines and in conjunction with the COR on the Contract.

4. Calibration/Certification Procedures: Certifiers Instrument Calibration: Certificates of

Calibration substantiating NIST (National Institute of Standards & Technology) traceability annual compliance with requirements, and minimum sensitivities of instruments used in

conducting testing in accordance with national Sanitation Standard No. 49; and ISO Standard

146447; or alternate standards as identified by the contractor.

D. SPECIFIC MANDATORY TASKS AND ASSOCIATED DELIVERABLES

Semi-Annual Environmental Sampling, Fingertip testing and Results Reporting: The contractor shall provide the specific deliverables described below within the performance period stated in Section A.4 of this SOW.

Work will be performed at:

1. West Palm Beach VAMC 7305 North Military Trail, West Palm Beach, FL 33410

SCHEDULE FOR DELIVERABLES

Unless otherwise specified, the number of draft copies and the number of final copies shall be the same. If for any reason any deliverable cannot be delivered within the scheduled time frame, the contractor is required to explain why in writing to the CO, including a firm commitment of when the work shall be completed. This notice to the CO shall cite the reasons for the delay, and the impact on the overall project. The CO will then review the facts and issue a response, in accordance with applicable regulations. If deliverable cannot be delivered within the scheduled time frame, compensation may be taken from the contractor.

**TEST RESULTS:**

Results of the testing will be provided to the VA COR within 7 calendar days of completion. All test results must be provided in both hard copy format through the U.S Postal mail and by confirmed e-mail PDF or WORD Format to the VA COR.

**ADVERSE TEST RESULTS:** Additional tests may be required by the VAMC West Palm Beach in between normal cycle dates if adverse results are reported. These as needed additional tests will be added to the contract through future modifications.

CHANGES TO THE STATEMENT OF WORK

Any changes to this SOW shall be authorized and approved only through written

correspondence from the Contracting Officer. 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.

G. GOVERNMENT RESPONSIBILITIES

The government will work in concert with the Contractor to help enable completion of the work

of the contract.

I. TRAVEL

Travel reimbursement other than as itemized in the contractor s bid is not authorized.

H. CONTRACTOR EXPERIENCE REQUIREMENTS

The contractor shall be Certified Environmental Microbiology Laboratory - ISO/IEC

17025:2005 Accreditation.

I. CONFIDENTIALITY AND NONDISCLOSURE It is agreed that:

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 after the task order.

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.

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.

J. CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY language FOR

Inclusion into CONTRACTS, as appropriate 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.

ACCESS to VA INFORMATION AND VA INFORMATION SYSTEMS

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.

All contractors, subcontractors, and third-party servicers and associates working with VA

information is 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.

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.

Custom software development and outsourced operations must be 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.

The C & A requirements do not apply, and that a Security Accreditation Package is not

required. The contractor generated data is NOT VA sensitive information.

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

For information systems that are hosted, operated, maintained, or used on behalf of VA at

non-VA facilities, contractors/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 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.

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.

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.

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

the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program

Office can provide guidance on whether a new C&A would be necessary.

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.

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

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.

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.

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:

Vendor must accept the system without the drive;

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

VA must reimburse the company for media at a reasonable open market replacement cost at

time of purchase.

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;

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

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 preapproved

and described in the purchase order or contract. 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.

4. SECURITY INCIDENT INVESTIGATION

M. 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. 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. 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.

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. LIQUIDATED DAMAGES FOR DATA BREACH

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.

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.

Each risk analysis shall address all relevant information concerning the data breach, including

the following:

Nature of the event (loss, theft, unauthorized access);

Description of the event, including:

date of occurrence;

data elements involved, including any PII, such as full name, social security number, date of

birth, home address, account number, disability code;

Number of individuals affected or potentially affected;

Names of individuals or groups affected or potentially affected;

Ease of logical data access to the lost, stolen or improperly accessed data considering the

degree of protection for the data, e.g., unencrypted, plain text;

Amount of time the data has been out of VA control;

The likelihood that the sensitive personal information will or has been compromised (made

accessible to and usable by unauthorized persons);

Known misuses of data containing sensitive personal information, if any;

Assessment of the potential harm to the affected individuals;

Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy

Incidents, as appropriate; and

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.

t. 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:

Notification;

One year of credit monitoring services consisting of automatic daily monitoring of at least 3

relevant credit bureau reports;

Data breach analysis;

Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit

freezes, to assist affected individuals to bring matters to resolution;

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

Necessary legal expenses the subjects may incur to repair falsified or damaged credit records,

histories, or financial affairs.

6. TRAINING

u. 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:

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;

Successfully complete the VA Cyber Security Awareness and Rules of Behavior training and

annually complete required security training;

Successfully complete the appropriate VA privacy training and annually complete required

privacy training; and

Successfully complete any additional cyber security or privacy training, as required for VA

personnel with equivalent information system access [to be defined by the VA program official

and provided to the contracting officer for inclusion in the solicitation document e.g., any role based

information security training required in accordance with NIST Special Publication 800-

16, Information Technology Security Training Requirements.]

The contractor shall provide to the contracting officer 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 the

training and documents are complete.

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.