CONSTRUCTION SCOPE OF WORK

Install ID Concrete Pad

Veterans Affairs Southern Nevada Healthcare System (VASNHS)

1. PROJECT IDENTIFICATION

Project Title:	Install ID Concrete Pad
Project Number:	**593-26-104**
Project Location:	**Storage Yard**
	VA Southern Nevada Healthcare System (VASNHS)
	6900 N Pecos Rd, North Las Vegas, NV 89086

2. PROJECT DESCRIPTION

This project will install a 90' x 61' 4" concrete slab to support two (2) 30' x 40' (ea 1200 SF) storage for Interior Design (ID). The slab will include required utility runs and grounding to support the storage units. The storage will be a conditioned tuff shed (or similar type structure) with underground electrical connection, a personnel single door, and aluminum roll up door.

3. PROJECT OBJECTIVES

Contractor shall provide all labor, materials, equipment, and administrative support necessary to complete the project. Contractor shall plan, schedule, and supervise for completion of the contract.

4. PROJECT REQUIREMENTS

1. Locate existing utilities before start of construction and protect existing utilities to remain during and/or after construction.
2. Subgrade preparation shall be made to the required depth and to a width that will permit the installation and bracing of the forms. The subgrade shall be shaped and compacted to a firm, even surface in conformity with existing grade. All soft and yielding material shall be removed and replaced with 12" thick Class 2 Aggregate Base and shall then be compacted to 95% relative compaction.
3. Set forms, install reinforcing steel at 12" on center each way and dowels at 18" on center, pour and finish 4" thick storage pad as indicated on Location Plan.
4. Hydrovac UG electrical trench ensuring pathway does not interfere with concrete footings. Install two (2) 2" RGC above ground and PVC Schedule 40 Pipe underground electrical pathway and a pull wire in one of the conduits. Provide two (2) 125 Amp breaker at existing electrical source and a Christy box.

5. Install UFER Ground.
6. Install 8’ copper ground rod inside ground rod box 10-1/4” I.D. x 12” (Christy – G3) with label cover “GROUND ROD.” Connect to storage container electrical panel.
   a. (4) x50 L Brackets 1/2" x 1/2" 16 Gage x 100 Stainless Steel Self Drilling Screws #8 1/2"
   b. (2) #12 1” Self-Drilling Screws Stainless Steel (Pack of 50)
   c. (4) 1 7/8” x 1 3/4" X 8’ Aluminum Side Post
   d. (8) 1 3/4" x 1 7/8” Side Post Flat Cap
   e. (8) 5” x 1.75” 8’ Aluminum Gate Frame
   f. (16) 1.75” x 5” Flat Gate Frame Cap
   g. (16) 2 1/32” x 5/32” x 8’ Aluminum Gate Frame Cover
   h. (2) 1.75” x 3/4” x 8’ Aluminum Gate Stopper
   i. (10) Black Hinge-Self Close with x 10 #10 screws for gates
   j. (6) #8 1/2” Self-Drilling Screws Stainless Steel (Pack of 100)
   k. (4) Black 12” cane bolt for gate
   l. (2) Sargent 70-10XG04-LL Heavy Duty Storeroom Lever Lockset, SFIC Core with A keyway, 7-pin
7. Contractor to verify existing project site conditions and square footages on plans. Immediately notify Contracting Officer in writing of any conflicting information from Specs and Drawings.

5. GOVERNMENT FURNISHED ITEMS

VASNHS will provide the following to the Contractor after contract award:

Item Description	Provided	Format
Project Drawings	With SOW	Separate PDF Doc
As-Built Drawings	As requested	AutoCAD/PDF Files
Specifications	With SOW	PDF

6. QUALITY ASSURANCE/QUALITY CONTROL

A. To reduce construction errors and omission, the Contractor shall develop and execute a QA/QC plan that demonstrates their proposed project plans and specifications have gone through a rigorous, thorough review and coordination effort with a minimum of three (3) phases of inspection/control procedures.
B. Within **ten (10) Federal workdays** after receipt of Notice to Proceed (NTP), the Contractor shall prepare and submit the following project-specific plans to include Contractor’s QA/QC representative for approval by the Contracting Officer’s Representative (COR) during the construction phase:
   1. Construction Safety Plan
   2. Environmental Protection Plan

3. Fire Safety Plan
4. Quality Control Plan
5. Waste Management Plan

C. Each task shall be initialed and dated by the Contractor's responsible team member.
D. The QA/QC personnel shall not perform any actual construction work.

7. SUBMITTALS

Provide submittals per Section 01 33 23 of the attached Specifications within **ten (10) Federal workdays** after receipt of NTP.

8. GOVERNMENT REVIEW OF SUBMITTALS and RFIs

A. VA review period for all Contractor submittals is **fifteen** (**15) Federal workdays**.
B. VA review period for all RFIs is **ten (10) Federal workdays.**

9. CONSTRUCTION COORDINATION

A. The Contractor shall coordinate all work with COR in accordance with the Specifications 01 00 00, General Requirements.
B. The Contractor shall prepare meeting agendas and submit meeting minutes after all coordination meetings.
C. Pre-Final and Final Inspections:
   I. The Contractor shall prepare punch lists if needed and schedule a pre-final walkthrough with the COR once substantial completion of each work location is achieved. After the pre-final walkthrough, the VA will submit its own punch list if needed.
   II. Once Contractor has completed or resolved all punch list items, the contractor shall schedule a final walkthrough with the COR.
   III. Required documentation:
      a. Contractor's punch list and confirmation of completion.
      b. Confirmation of VA's completed punch list.
      c. Factory representative certification.
      d. All warranty, operations and maintenance manuals.

10. SCHEDULES

A. Project Schedule: The Contractor shall provide a schedule that estimates the length of time to prepare site, pour concrete slab and install new shipping container with electrical connections and aluminum screen wall fence with gates The Contractor shall

prepare the estimated schedule per specifications 01 32 16, Project Schedules and deliver one hard copy and an electronic copy to the COR and the CO within 14 calendar days of NTP. The contractor shall maintain this schedule and provide updates as needed via e-mail to the COR and the CO.

B. 3-Week Look Ahead Schedule: The contractor shall provide a 3-Week Lookahead schedule at each weekly Construction Progress meeting. The schedule shall show the actual construction work performed on previous week and the 3 weeks of future work scheduled for a total of 4 weeks.

11. SECURITY REQUIREMENTS

A. The Certification & Accreditation (C&A) Requirements do not apply, and a Security Accreditation Package is not required.
B. Contractors do not need and shall not be allowed access to any VA personnel's' or VA patients' Personal Health Information (PHI) or Personally Identifiable Information (PII) in the performance of the requirements of the Statement of Work (SOW) requirements. Additionally, the Contractor does not need and shall not be allowed access to VA sensitive information in the performance of the requirements of the SOW requirements.
C. Contractor shall not connect contractor-owned IT devices (laptop computers or remote connections from a Contractor system) to a VA internal trusted (non-public) network. The Certification and Accreditation requirements do not apply, and a Security Accreditation Package is not required.
D. Contractors, Contractor's personnel, subcontractors, and subcontractors' personnel shall be subject to the same Federal laws, regulations, standards and VA Directives and Handbooks as VA and VA personnel in regard to information and information system security.

12. SECURITY REQUIREMENTS – FOR REFERENCE ONLY

SECURITY REQUIREMENTS FOR UNCLASSIFED INFORMATION TECHNOLOGY SECURITY RESOURCES

a. The contractor and their personnel shall be subject to the same Federal laws, regulations, standards and VA polices as VA personnel, regarding information and information system security. These include, but are not limited to Federal Information Security Management Act (FISMA), Appendix III of OMB Circular A-130, and guidance and standards, available from the Department of Commerce's National Institute of Standards and Technology (NIST). This also includes the use of common security configuration available from NIST's Web site at: http://checklists.nist.gov.

b. To ensure that appropriate security controls are in place, contractors must follow the procedures set forth in "VA Information and Information System Security/Privacy Requirements for IT Contractors" located at the following site: http://www.iprm.oit.va.gov.

c. These provisions shall apply to all contracts in which VA sensitive information is stored, generated, transmitted, or exchanged by VA, a contractor, subcontractor or a third-party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor/subcontractor's electronic information system(s) operating for or on the VA behalf.

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 withVA 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.

e. The contractor or subcontractor must notify the COR 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 COR must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

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 thecontractors/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 COR 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. In accordance with 45 CFR 164.502(e), the Privacy Rule includes exceptions to the Business Associate Standard. This requirement meets the exception and does not require a Business Associate agreement in order for Covered Entity to disclose Protected Healthcare Information to the contractor for treatment.

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. The records created in accordance with this contract belong to the VASNHS and should be returned to the VASNHS and/or destroyed in accordance with VHA RCS 10-1. Destruction should only occur with advance notice and guidance from the Records Management Officer at the VASNHS. Records shall be safeguarded in accordance with the Privacy Act, Health Insurance Portability and Accountability Act (HIPAA) and the VASNHS Release of Information Unit. Patient Medical information is considered privileged and shall not be disclosed or revealed in any way without prior written permission from the VA Chief, Health Information Management Section.

k. The Contractor shall only release medical information obtained during the course of this contract to those VA staff members involved in the necessary management and treatment of that individual patient. Patient list and name of patients are considered privileged information and shall not be disclosed or revealed in any way for use outside the Contractor without prior written permission from the referring VA Chief of Staff. Veterans requesting copies of medical information generated by the contractor will be referred to the VASNHS Release of Information Unit.

l. 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 VASNHS Release of Information Unit for response.

m. 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 VASNHS Release of Information Unit for response.

n. 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 6500.1requirements. This must be completed within 30 days of termination of the contract.

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

Ensure that a Contractor Security Control Assessment (CSCA) is completed within 30 days of contract approval and yearly on the renewal date of the contract.

Ensure that the CSCA is sent to the ISO and the OCS Certification Program Office for review to ensure that appropriate security controls are being implemented in service contracts.

Ensure a copy of the CSCA is maintained in the Security Management and Reporting Tool (SMART) database. COR will provide a copy of the completed CSCA to ISO for uploading into SMART database.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA):

Contractor shall take reasonable measures to ensure patient privacy and confidentiality. The contractor agrees to take all reasonable precautions to safeguard patient information from unauthorized access or modification, in both electronic and hard-copy formats. This includes not only electronic security measures such as “strong” user passwords on computer systems, but also physical barriers to prevent unauthorized use of computer work-stations; that hard copy patient files are in secured lockable areas, that files are in lockable cabinets, that the cabinets can in fact be locked, i.e., keys are available, and the locking mechanisms work properly. This precaution also includes the proper transfer of patient information via electronic means, such as faxing or system to system transmission.

That only the minimum necessary patient information is used to provide appropriate service to the correct patient.

That the undersigned understands that all parties are bound by the requirements of the “Health Insurance Portability and Accountability Act of 1996” which provide guidance on the protection of patient privacy and confidentiality. This Act mandates that all government agencies, and those bodies with whom they contract, must be in compliance with the directives of the Act.

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.

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 $37.50 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.

SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

TRAINING

Contractor/subcontractor employees requiring access to VA information shall complete privacy training annually as required for covered entities under the HIPAA.

The COR shall ensure employees complete training within 1 week of the initiation of the contract and annually thereafter, as required.

Failure to complete the mandatory annual training 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.

13. SITE VISITS

Contractor shall visit the work site at VASNHS prior to commencing the construction. The Contractor shall survey project site to the extent required to confirm existing conditions and equipment currently installed. New construction materials and equipment to match existing unless variation submittal is approved by CO.

14. PERIOD OF PERFORMANCE

The Period of Performance will begin upon issuance of a Notice to Proceed from VA Contracting. The project requires all tasks defined within this SOW to be completed within **180 Calendar days** after NTP.

15. HOURS OF WORK

Work hours are 7:00am – 4:00pm, Monday thru Friday. All work performed shall be coordinated and scheduled thru the COR. Any work outside of work hours must be coordinated and approved through the COR.

16. OTHER PERTINENT INFORMATION OR SPECIAL CONSIDERATIONS

A. The Contractor is responsible for ensuring all equipment used by the Contractor on VASNHS properties has been inspected and is safe for use. The Contractor's personnel shall be licensed, certified, and trained as required to operate this equipment.
B. The Contractor shall be responsible for the inspection and storage of contractor equipment and materials that will be used in the performance of this contract. The Contractor shall coordinate with the VA COR to determine storage locations and laydown area(s).

17. RISK CONTROL

A. The Contractor shall ensure all construction materials and equipment are stored and secured in a manner to limit theft or damage by weather, other contractors, staff, patients, etc.
B. The work area shall be cleaned and made safe at end of each workday.

18. PRICING

A. Contractor shall provide a fee for the required services using the format applicable to the Request for Proposal document issued by the CO.
B. Contractor shall submit a detailed Schedule of Values for approval by CO required for invoice payments.

19. NATIONAL HOLIDAYS:

New Year's Day	January 1
Martin Luther King's Birthday	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Juneteenth National Independence Day	June 19
Independence Day	July 4
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veterans Day	November 11
Thanksgiving Day	Fourth Thursday in November
Christmas Day	December 25

When a holiday falls on a Sunday, the following Monday shall be observed as a legal holiday by U.S. Government agencies. When a holiday falls on a Saturday, the preceding Friday shall be observed as a legal holiday by U.S. Government agencies. Also included would be any other day specifically declared by the President of the United States as a National Holiday. Reference (Federal Holidays (opm.gov)

20. REFERENCE STANDARDS

See specifications sections 01 42 19, Reference Standards.

21. INNOVATION

Requirements indicated are not intended to limit innovative service delivery of the contractor. The Government will consider variations from the Statement/Scope of Work (SOW), if the proposed change is within the schedule and budget limitations, meets the objectives for the

project, and results in an improved outcome. The Government must approve all proposed changes to the SOW.

END of STATEMENT OF WORK