

The Pittsburgh VA Medical Center, University Drive C, Pittsburgh, PA 15240 has a Video Recording System requirement as per Statement Of Need (SON) and Statement Of Work (SOW) listed below.

### **Statement of Need**

The Closed Circuit Television (CCTV) system at VA Pittsburgh Healthcare System (VAPHS) is a critical element of patient and staff safety as well as physical security monitored by medical center staff and VA Police. December 2016 reports indicate that 48% of all CCTV cameras at VAPHS are malfunctioning (357 of 745 cameras). The problem is worse in two critical areas monitored by Police: University Drive Emergency Department (73% failure rate) and Heinz Campus Domiciliaries (70% failure rate). The malfunctions are typically intermittent and may be due to either a video loss from the camera, failure of recording equipment to store video or various computer network factors. System malfunction creates a potential safety hazard for patients as well as staff due to lack of ability for medical staff and Police to observe activities in critical areas including Emergency Department, high-risk patient areas, pharmacy drug storage and other critical medical center areas.

Hard drive replacement is one component of an overall project to improve the reliability of the CCTV system at VAPHS. Based on a CCTV system evaluation utilizing Pelco expert services, VA OI&T staff, and Police and Facilities Management staff, system improvements will include upgrade the NSM5200 system manager units, upgrade storage capacities on existing NSM5200's, consolidate VLAN's, reallocate Endura servers and NSM's to properly controlled environments, update network settings for Endura requirements, replace 18 DVR5100's with NET5516 encoders, replace 18 EOL NET5300B with NET5516 encoders, and update firmware on IP cameras that are not responding. Following system hardware upgrade, VA OI&T staff will reconfigure the system on the network to reduce the number of VLANs and streamline communications. The combination of hardware upgrades and network configuration improvements will restore reliability to the CCTV system at VAPHS.

### **Statement of Work**

The contractor shall provide all labor, material and equipment necessary to perform work as follows:

1. Relocate all NSM5200 units from current locations such as the UD-B1-AN303 Rack Room and other IT closets throughout Heinz (HZ) and University Drive (UD) campuses to either the HZ Building 32 Data Center or UD 5th Floor Data Center. Note that this work will require close coordination with VA OI&T.
2. Replace existing hard drives (Quantity of 204) in NSM5200 equipment. Program and test the equipment with the new hard drives.
3. Provide complete documentation for all work including device configuration information, physical location, connections, licenses and software.

The contractor shall coordinate the installation and testing with the VA O&IT, Police and Facilities Management Departments. The project COR will provide contact information for VA Departments.

The work shall be performed at the University Drive and Heinz campuses of VAPHS. Work will be performed on days mutually agreed upon by the contractor and VAPHS COR during normal business hours: Monday-Friday, 7:00 AM – 3:30 PM unless other work hours are mutually agreed upon by VAPHS COR and the contractor.

### **Data Security and Privacy**

Contractor must comply with COR instruction to ensure compliance with physical security policies. A compliant ID badge must be worn by Contractors at all times while on VA premises.

An MBI is required if contractor personnel will need unescorted access to sensitive IT areas (a BI is required if unescorted access is required to the data center or a server room). Otherwise, contractor must be escorted by authorized VA OI&T personnel at all times while performing work in sensitive IT areas.

The following items from 6500.6 are here-by included in the contract:

- Appendix C: Paragraphs #6a,b, #7(all), #9(all)
- Each contractor and subcontractor employee requiring unescorted access to sensitive areas must read and sign Appendix D, Contractor Rules of Behavior.

Contractor may not have access to any VA sensitive information. Contractor may only access devices on the VA network secured by VLANs and ACL's as required under this contract. Contractor owned computer equipment including laptops are not permitted to be connected to the VA network.

Contractor may not remove any equipment which stores data, i.e. hard drives, etc, from VA property.

All contractors working on-site must complete “VA Privacy and Information Security Awareness and Rules of Behavior” training prior to the performance of the contract and annually thereafter. Training must be completed in VA’s TMS system and tracked by the COR.

### **DISCLAIMER**

This RFI is issued solely for information and planning purposes only and does not constitute a solicitation. All information received in response to this RFI that is marked as proprietary will be handled accordingly. In accordance with FAR 15.201(e), responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this RFI.

End of Document