

ATTACHMENT E - VA SPECIFICATION – SECTION 28 13 16 PHYSICAL ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT

SECTION 28 13 16 PHYSICAL ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT

SPEC WRITER NOTE: Delete between //___//if not applicable to project. Also delete any other item or paragraph not applicable in the section and renumber the paragraphs.

PART 1 – GENERAL

1.1 DESCRIPTION

- A. This section specifies the finishing, installation, connection, testing and certification of a complete and fully operation Physical Access Control Database Management System, hereinafter referred to as the PACMS.
- B. This Section includes a Physical Security Access System Database Management consisting of database management software. Requirements for hardware supporting database management are described in Section 28 13 00 PHYSICAL ACCESS CONTROL, Part 2.

1.2 RELATED WORK

SPEC WRITER NOTE: Delete any item or paragraph not applicable in the section and renumber the paragraphs.

- A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.
- B. Section 28 05 00 - COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. Requirements for general requirements that are common to more than one section in Division 28.
- C. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.
- D. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding and bonding.
- E. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.

- F. Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS. For requirements for commissioning and systems readiness checklists.
- G. Section 28 13 00 - PHYSICAL ACCESS CONTROL SYSTEM. Requirements for physical access control system.
- H. Section 28 13 53 - SECURITY ACCESS DETECTION. Requirements for screening of personnel and shipments.
- I. Section 28 16 00 - INTRUSION DETECTION SYSTEM (IDS). Requirements for alarm systems.
- J. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.
- K. Section 28 26 00 - ELECTRONIC PERSONAL PROTECTION SYSTEM (EPPS). Requirements for emergency and interior communications.

1.3 QUALITY ASSURANCE

- A. The Contractor shall be responsible for providing, installing, and the operation of the Access Control System and Database Management as shown. The Contractor shall also provide certification as required.
- B. The security system shall be installed and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the security system is stand-alone or a part of a Information Technology (IT) computer network.
- C. The Contractor or security sub-contractor shall be a licensed security Contractor as required within the state or jurisdiction of where the installation work is being conducted.
- D. The manufacturers of all hardware and software components employed in the SMS shall be established vendors to the access control/security monitoring industry for no less than five (5) years and shall have successfully implemented at least 5 systems of similar size and complexity.
- E. Contractor / Integrator Qualifications
 - 1. The security system integrator shall have been regularly engaged in the installation and maintenance of integrated access control systems and have a proven track record with similar systems of the same size, scope, and complexity.
 - 2. The security system integrator shall supply information attesting to the fact that their firm is an authorized product

integrator certified with the SMS. A minimum of one technician shall be a installer certified by the SMS manufacturer.

3. The security system integrator shall supply information attesting to the fact that their installation and service technicians are competent factory trained and certified personnel capable of maintaining the system and providing reasonable service time.
4. The security system integrator shall provide a minimum of three (3) references whose systems are of similar complexity and have been installed and maintained by the security system integrator in the last five (5) years.
5. There shall be a local representative and factory authorized local service organization that shall carry a complete stock of parts and provide maintenance for these systems.

F. Service Qualifications: There shall be a permanent service organization maintained or trained by the manufacturer which will render satisfactory service to this installation within // four // // eight // hours of receipt of notification that service is needed. Submit name and address of service organizations.

1.4 SUBMITTALS

SPEC WRITER NOTE: Delete and/or amend all paragraphs and sub-paragraphs and information as needed to ensure that only the documentation required is requested per the Request for Proposal (RFP).

- A. Submit below items in conjunction with Master Specification Sections 01 33 23, SHOP DRAWINGS, PRODUCT DATA, AND SAMPLES, and Section 02 41 00, DEMOLITION.
- B. Provide certificates of compliance with Section 1.3, Quality Assurance.
- C. Provide a pre-installation and as-built design package in both electronic format and on paper, minimum size 48 x 48 inches (1220mm x 1220mm); drawing submittals shall be per the established project schedule.
- D. Pre-installation design and as-built packages shall include, but not be limited to:
 1. Index Sheet that shall:

- a. Define each page of the design package to include facility name, building name, floor, and sheet number.
 - b. Provide a list of all security abbreviations and symbols.
 - c. Reference all general notes that are utilized within the design package.
 - d. Specification and scope of work pages for all security systems that are applicable to the design package that will:
 - 1) Outline all general and job specific work required within the design package.
 - 2) Provide a device identification table outlining device Identification (ID) and use for all security systems equipment utilized in the design package.
2. Drawing sheets that will be plotted on the individual floor plans or site plans shall:
- a. Include a title block as defined above.
 - b. Define the drawings scale in both standard and metric measurements.
 - c. Provide device identification and location.
 - d. Address all signal and power conduit runs and sizes that are associated with the design of the electronic security system and other security elements (e.g., barriers, etc.).
 - e. Identify all pull box and conduit locations, sizes, and fill capacities.
 - f. Address all general and drawing specific notes for a particular drawing sheet.
3. A riser drawing for each applicable security subsystem shall:
- a. Indicate the sequence of operation.
 - b. Relationship of integrated components on one diagram.
 - c. Include the number, size, identification, and maximum lengths of interconnecting wires.
 - d. Wire/cable types shall be defined by a wire and cable schedule. The schedule shall utilize a lettering system that will correspond to the wire/cable it represents (example: A = 18 AWG/1 Pair Twisted, Unshielded). This schedule shall also provide the manufacturer's name and part number for the wire/cable being installed.
4. A system drawing for each applicable security system shall:

- a. Identify how all equipment within the system, from main panel to device, shall be laid out and connected.
 - b. Provide full detail of all system components wiring from point-to-point.
 - c. Identify wire types utilized for connection, interconnection with associate security subsystems.
 - d. Show device locations that correspond to the floor plans.
 - e. All general and drawing specific notes shall be included with the system drawings.
5. A schedule for all of the applicable security subsystems shall be included. All schedules shall provide the following information:
- a. Device ID.
 - b. Device Location (e.g. site, building, floor, room number, location, and description).
 - c. Mounting type (e.g. flush, wall, surface, etc.).
 - d. Power supply or circuit breaker and power panel number.
 - e. In addition, for the CCTV Systems, provide the camera ID, camera type (e.g. fixed or pan/tilt/zoom (P/T/Z), lens type (e.g. for fixed cameras only) and housing model number.
6. Detail and elevation drawings for all devices that define how they were installed and mounted.
- E. Pre-installation design packages shall be reviewed by the Contractor along with a VA representative to ensure all work has been completed. All reviews shall be conducted in accordance with the project schedule. There shall be four (4) stages to the review process:
- 1. 35 percent
 - 2. 65 percent
 - 3. 90 percent
 - 4. 100 percent
- F. Provide manufacturer security system product cut-sheets. Submit for approval at least 30 days prior to commencement of formal testing, a Security System Operational Test Plan. Include procedures for operational testing of each component and security subsystem, to include performance of an integrated system test.

- G. Submit manufacture's certification of Underwriters Laboratories, Inc. (UL) listing as specified. Provide all maintenance and operating manuals per Section 01 00 00, GENERAL REQUIREMENTS.

1.5 APPLICABLE PUBLICATIONS

SPEC WRITER NOTE: Delete first paragraph below if stand alone specs. Delete rest of the subparagraphs if section 280500 is provided with the project.

- //A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1//
- A. The publications listed below (including amendments, addenda, revisions, supplement, and errata) form a part of this specification to the extent referenced. The publications are referenced in the text by the basic designation only.
- B. American National Standards Institute (ANSI)/ Security Industry Association (SIA):
- AC-03.....Access Control: Access Control Guideline
Dye Sublimation Printing Practices for
PVC Access Control Cards
- TVAC-01.....CCTV to Access Control Standard - Message
Set for System Integration
- C. American National Standards Institute (ANSI)/ International Code Council (ICC):
- A117.1.....Standard on Accessible and Usable
Buildings and Facilities
- D. Department of Justice American Disability Act (ADA)
28 CFR Part 36.....2010 ADA Standards for Accessible Design
- E. Federal Communications Commission (FCC):
- (47 CFR 15) Part 15.....Limitations on the Use of Wireless
Equipment/Systems
- F. Government Accountability Office (GAO):
- GAO-03-8-02Security.....Responsibilities for Federally Owned and
Leased Facilities
- G. National Electrical Contractors Association
303-2005.....Installing Closed Circuit Television
(CCTV) Systems
- H. National Electrical Manufacturers Association (NEMA):

- 250-08.....Enclosures for Electrical Equipment (1000
Volts Maximum)
- I. National Fire Protection Association (NFPA):
- 70-11..... National Electrical Code
- J. Underwriters Laboratories, Inc. (UL):
- 294-99.....The Standard of Safety for Access Control
System Units
- 305-08.....Standard for Panic Hardware
- 639-97.....Standard for Intrusion-Detection Units
- 752-05.....Standard for Bullet-Resisting Equipment
- 827-08.....Central Station Alarm Services
- 1076-95.....Standards for Proprietary Burglar Alarm
Units and Systems
- 1981-03.....Central Station Automation System
- 2058-05.....High Security Electronic Locks
- K. Homeland Security Presidential Directive (HSPD):
- HSPD-12.....Policy for a Common Identification
Standard for Federal Employees and
Contractors
- L. Federal Information Processing Standards (FIPS):
- FIPS-201-1.....Personal Identity Verification (PIV) of
Federal Employees and Contractors
- M. National Institute of Standards and Technology (NIST):
- IR 6887 V2.1.....Government Smart Card Interoperability
Specification (GSC-IS)
- Special Pub 800-37.....Guide for Applying the Risk Management
Framework to Federal Information Systems
- Special Pub 800-63.....Electronic Authentication Guideline
- Special Pub 800-73-3....Interfaces for Personal Identity
Verification (4 Parts)
-Pt. 1- End Point PIV Card Application
Namespace, Data Model & Representation
-Pt. 2- PIV Card Application Card Command
Interface
-Pt. 3- PIV Client Application Programming
Interface
-Pt. 4- The PIV Transitional Interfaces &
Data Model Specification

- Special Pub 800-76-1....Biometric Data Specification for Personal Identity Verification
- Special Pub 800-78-2....Cryptographic Algorithms and Key Sizes for Personal Identity Verification
- Special Pub 800-79-1....Guidelines for the Accreditation of Personal Identity Verification Card Issuers
- Special Pub 800-85B-1...DRAFTPIV Data Model Test Guidelines
- Special Pub 800-85A-2...PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-3 compliance)
- Special Pub 800-96.....PIV Card Reader Interoperability Guidelines
- Special Pub 800-104A....Scheme for PIV Visual Card Topography
- Special Pub 800-116.....Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
- N. International Organization for Standardization (ISO):
- 7810.....Identification cards - Physical characteristics
- 7811.....Physical Characteristics for Magnetic Stripe Cards
- 7816-1.....Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics
- 7816-2.....Identification cards - Integrated circuit cards - Part 2: Cards with contacts - Dimensions and location of the contacts
- 7816-3.....Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols
- 7816-4.....Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods
- 7816-10.....Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange

- 14443.....Identification cards - Contactless
integrated circuit cards; Contactless
Proximity Cards Operating at 13.56 MHz in
up to 5 inches distance
- 15693.....Identification cards -- Contactless
integrated circuit cards - Vicinity
cards; Contactless Vicinity Cards
Operating at 13.56 MHz in up to 50 inches
distance
- 19794.....Information technology - Biometric data
interchange formats

O. Uniform Federal Accessibility Standards (UFAS) 1984

P. Section 508 of the Rehabilitation Act of 1973

1.6 WARRANTY OF CONSTRUCTION.

- A. Warrant PACMS work subject to the Article "Warranty of Construction" of FAR clause 52.246-21 and Section 280500.
- B. Demonstration and training shall be performed prior to system acceptance.

PART 2 - PRODUCTS

Spec Note: Delete or amend all paragraphs and sub-paragraphs as needed to ensure that only the equipment required per the Request for Proposal (RFP) is provided.

2.1 SYSTEM DATABASE

- A. Database and database management software shall be HSPD-12 and FIPS compliant. Database and database management software shall define and modify each point in database using operator commands. Definition shall include parameters and constraints associated with each system device.
- B. Database Operations:
 - 1. System data management shall be in a hierarchical menu tree format, with navigation through expandable menu branches and manipulated with use of menus and icons in a main menu and system toolbar.
 - 2. Navigational Aids:

- a. Toolbar icons for add, delete, copy, print, capture image, activate, deactivate, and muster report.
 - b. Point and click feature to facilitate data manipulation.
 - c. Next and previous command buttons visible when editing database fields to facilitate navigation from one record to the next.
 - d. Copy command and copy tool in the toolbar to copy data from one record to create a new similar record.
- 3. All data entry shall be automatically checked for duplicate and illegal data and shall verify that data are in a valid format.
 - 4. Provide a memo or note field for each item that is stored in database, allowing the storing of information about any defining characteristics of the item. Memo field is used for noting the purpose the item was entered for, reasons for changes that were made, and the like.

C. File Management:

- 1. Provide database backup and restoration system, allowing selection of storage media, including hard discs, optical media, flash drives, and designated network resources.
- 2. Provide manual and automatic mode of backup operations. The number of automatic sequential backups before the oldest backup becomes overwritten; FIFO mode shall be operator selectable.
- 3. Backup program shall provide manual operation from any PC on the LAN and shall operate while system remains operational.

D. Database Segmentation:

- 1. The System shall employ advanced database segmentation functionality. Each segment shall be allowed to have its own unique set of cardholders, hardware, and system parameters including access control field hardware, timezones, access levels, etc., which shall allow System Administrators to expand upon current hardware constraints. As such, only credentials that are assigned access levels to card readers in a segment need to be downloaded to the Data Gathering Panels in that segment.
- 2. Cardholders shall be allowed to belong to one segment, many segments, or all segments.

3. The database segmentation functionality shall also provide a capability to object records in the system, where segment System Administrators and Operators can only view, add, modify, delete, and manipulate cardholders, system parameters and access control field hardware that belong to their respective segments.
4. System Administrators and System Operators shall be assigned the segments they are allowed to view and control. System Administrators and System Operators may be assigned to more than one segment and a segment may be assigned to more than one System Administrator and System Operator. A one-to-many relationship shall exist for System Administrators and System Operators with respect to segments. The SYSTEM shall support a minimum of [65,000] <insert number> segments.

E. Bi-Directional Data Exchange

1. The System shall support a real time, bi directional data interface to external databases such as Human Resources, Time and Attendance, Food Service Systems. The interface shall allow data to be imported into or exported out of the SYSTEM in real time or in a batch mode basis. Data used for import shall be retrieved directly from an external database or through an import file. Data provided for export shall be applied directly to an external database or through an export file. Any data shall be imported or exported including image data. The file used for import or created by export shall have the ability to be structured in a wide variety of ways, but shall always be in ASCII text format.
2. The System shall also support a one step download and distribution process of cardholder and security information from the external database to the SYSTEM database, all the way down to the Intelligent Field Controller (ISC) database. This shall be a guaranteed process, even if the communication path between the SYSTEM database server and the ISC is broken. If the communication path is broken, the data shall be stored in a temporary queue and shall be automatically downloaded once the communication path is restored.

F. Database connectivity:

1. The SMS database shall support open direct database connectivity for importing cardholder and card ID data from external systems and/or database applications. The PACS SMS shall facilitate interfacing by providing the following capabilities:
 - a. Real time and batch processing of data via ODBC, JDBC or OLE DB over a network connection.
 - b. Insert, update, and delete record information.
 - c. Automatic download of data to control panels (data gathering panels) based on database changes.
 - d. Provide audit trail in the operator history/archive database for all database changes initiated by the interface.

G. Operator Passwords:

1. Software shall support up to [32,000] <insert number> individual system operators, each with a unique password.
2. Operator Password: [One to eight alphanumeric characters] <Insert password characteristic>.
3. Allow passwords to be case sensitive.
4. Allow use of Single sign-off (SSO) password.
5. Passwords shall not be displayed when entered.
6. Provide each password with a unique and customizable password profile, and allow several operators to share a password profile. Include the following features in the password profile:
 - a. Allow for at least [32,000] <Insert number> operator password profiles.
 - b. Predetermine the highest-level password profile for access to all functions and areas of program.
 - c. Allow or disallow operator access to any program operation, including the functions of View, Add, Edit, and Delete.
 - d. Restrict which doors an operator can assign access to.
7. Operators shall use a user name and password to log on to system.
 - a. This user name and password is used to access database areas and programs as determined by the associated profile.
8. Make provision to allow the operator to log off without fully exiting program. User may be logged off but program will

remain running while displaying the login window for the next operator.

SPEC WRITER NOTE: Edit between // as required by the project.

- H. Access Card/Code Operation and Management: Access authorization shall be by card /, by a manually entered code (PIN), by a combination of both (card plus PIN), by a biometric, by combination of PIN and biometric/.
1. Access authorization shall verify the card or card-and-PIN validation, and the access level (time of day, day of week, date), anti-passback status, and number of uses last.
 2. Use data-entry windows to view, edit, and issue access levels. Access authorization entry management system shall maintain and coordinate all access levels to prevent duplication or the incorrect creation of levels.
 3. Allow assignment of multiple cards/codes to a cardholder.
 4. Allow assignment of at least four access levels for each Location to a cardholder. Each access level may contain any combination of doors.
 5. Each door may be assigned four time zones.
 6. Access codes may be up to 11 digits in length.
- SPEC WRITER NOTE: Feature in first subparagraph below helps speed data entry.
7. Software shall allow the grouping of locations so cardholder data can be shared by all locations in the group.
 8. Visitor Access: Issue a visitor badge, without assigning that person a card or code, for data tracking or photo ID purposes.
 9. Cardholder Tracing: Allow for selection of cardholder for tracing. Make a special audible and visual annunciation at control station when a selected card or code is used at a designated code reader. Annunciation shall include an automatic display of the cardholder image.
 10. Allow option for each cardholder to be given either an unlimited number of uses or a number from 1 to 9998 that regulates the number of times the card can be used before it is automatically deactivated.
 11. Provide for cards and codes to be activated and deactivated manually or automatically by date. Provide for multiple deactivate dates to be preprogrammed.

I. Security Access Integration:

1. Photo ID badging and photo verification shall use same database as the security access and may query data from cardholder, group, and other personal information to build a custom ID badge.
2. The SMS shall provide a means for manually importing and exporting selected data in XML format. This mechanism shall support the import and export of any and all classes or types of data in the system. Specific data validation and logging requirements shall be met.
3. The system shall also support importing from CSV files.
4. The SMS shall provide an automated import mechanism (preferably XML-based). This mechanism shall support the import of most classes or types of data into the system. Specific data validation and logging requirements shall be met.
5. The SMS shall provide a Data Mapping feature that provides field mapping information using the XSLT file based on the input data or an external XSLT file.
6. Automatic or manual image recall and manual access based on photo verification shall also be a means of access verification and entry.
7. System shall allow sorting of cardholders together by group or other characteristic for a fast and efficient method of reporting on, and enabling or disabling, cards or codes.

J. Key control and tracking shall be an integrated function of cardholder data.

1. Provide the ability to store information about which conventional metal keys are issued and to whom, along with key construction information.
2. Reports shall be designed to list everyone that has possession of a specified key.

K. Operator Comments:

1. With the press of one appropriate button on toolbar, the user shall be permitted to make operator comments into history at anytime.
2. Automatic prompting of operator comment shall occur before the resolution of each alarm.

3. Operator comments shall be recorded by time, date, and operator number.
4. Comments shall be sorted and viewed through reports and history.
5. The operator may enter comments in two ways; either or both may be used:
 - a. Manually entered through keyboard data entry (typed), up to 65,000 characters per each alarm.
 - b. Predefined and stored in database for retrieval on request.
6. System shall have a minimum of 999 predefined operator comments with up to 30 characters per comment.

L. Group:

1. Group names may be used to sort cardholders into groups that allow the operator to determine the tenant, vendor, contractor, department, division, or any other designation of a group to which the person belongs.
2. System software shall have the capacity to assign 1 of 32,000 group names to an access authorization.
3. Make provision in software to deactivate and reactivate all access authorizations assigned to a particular group.
4. Allow sorting of history reports and code list printouts by group name.

M. Time Zones:

1. Each zone consists of a start and stop time for 7 days of the week and three holiday schedules. A time zone is assigned to inputs, outputs, or access levels to determine when an input shall automatically arm or disarm, when an output automatically opens or secures, or when access authorization assigned to an access level will be denied or granted.
2. Up to four time zones may be assigned to inputs and outputs to allow up to four arm or disarm periods per day or four lock or unlock periods per day; up to three holiday override schedules may be assigned to a time zone.
3. Data-entry window shall display a dynamically linked bar graph showing active and inactive times for each day and holiday, as start and stop times are entered or edited.
4. System shall have the capacity for [2048] <Insert number> time zones for each Location.

N. Holidays:

1. Three different holiday schedules may be assigned to a time zone. Holiday schedule consists of date in format MM/DD/YYYY and a description. When the holiday date matches the current date of the time zone, the holiday schedule replaces the time zone schedule for that 24-hour period.
2. System shall have the capacity for [32,000] <Insert number> holidays.
3. Three separate holiday schedules may be applied to a time zone.
4. Holidays have an option to be designated as occurring on the designated date each year. These holidays remain in system and will not be purged.
5. Holidays not designated to occur each year shall be automatically purged from database after the date expires.

O. Access Levels:

1. System shall allow for the creation at least [32,000] <Insert number> access levels.
2. System shall allow for access to be restricted to any area by reader and by time. Access levels shall determine when and where an Identifier is authorized.
3. System shall be able to create multiple door and time zone combinations under same access level so that an Identifier may be valid during different time periods at different readers even if the readers are on the same Controller.

P. User-Defined Fields:

1. System shall provide a minimum of 99 user-defined fields, each with up to 50 characters, for specific information about each credential holder.
2. System shall accommodate a title for each field; field length shall be 20 characters.
3. A "Required" option may be applied to each user-defined field that, when selected, forces the operator to enter data in the user-defined field before the credential can be saved.
4. A "Unique" option may be applied to each user-defined field that, when selected, will not allow duplicate data from different credential holders to be entered.

5. Data format option may be assigned to each user-defined field that will require the data to be entered with certain character types in specific spots in the field entry window.
6. A user-defined field, if selected, will define the field as a deactivate date. The selection shall automatically cause the data to be formatted with the windows MM/DD/YYYY date format. The credential of the holder will be deactivated on that date.
7. A search function shall allow any one user-defined field or combination of user-defined fields to be searched to find the appropriate cardholder. The search function shall include search for a character string.
8. System shall have the ability to print cardholders based on and organized by the user-defined fields.

Q. Code Tracing:

1. System shall perform code tracing selectable by cardholder and by reader.
2. Any code may be designated as a "traced code" with no limit to how many codes can be traced.
3. Any reader may be designated as a "trace reader" with no limit to which or how many readers can be used for code tracing.
4. When a traced code is used at a trace reader, the access-granted message that usually appears on the monitor window of the Central Station shall be highlighted with a different color than regular messages. A short singular beep shall occur at the same time the highlighted message is displayed on the window.
5. The traced cardholder image (if image exists) shall appear on workstations when used at a trace reader.

R. Database and File Replication:

1. The Security Management System shall be capable of supporting database and file replication using [Microsoft SQL Server Replication Services and Microsoft File Replication Services] <insert database and file replication services> for providing distributed database replication across multiple PACS application servers allowing for system expansion and delivering N tiers of server redundancy.
2. Database and file replication shall not require any proprietary database or file replication software.

PART 3 - EXECUTION**3.1 INSTALLATION**

SPEC WRITER NOTE: Delete and/or amend this all paragraphs and sub-paragraphs to apply to only the equipment and devices that are being installed.

- A. System installation shall be in accordance with manufacturer and related documents and references, for each type of security subsystem designed, engineered and installed.
- B. All software shall be installed per the design package and the manufacturer's installation specifications.

3.2 TESTING AND TRAINING

- A. All testing and training shall be compliant with the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.
- B. Perform testing and system certification as outlined in section 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.
- C. The software shall be entered into the SMS computer systems and debugged. The Contractor shall be responsible for documenting and entering the initial database into the system. The Contractor shall provide the necessary blank forms with instructions to fill in all the required data information that will make up the database. The database shall then be reviewed by the Contractor and entered into the system. Prior to full operation, a complete demonstration of the computer real time functions shall be performed. A printed validation log shall be provided as proof of operation for each software application package. In addition, a point utilization report shall be furnished listing each point, the associated programs utilizing that point as an input or output and the programs which that point initiates.
- D. Upon satisfactory on line operation of the system software, the entire installation including all subsystems shall be inspected. The Contractor shall perform all tests, furnish all test equipment and consumable supplies necessary and perform any work as required to establish performance levels for the system in accordance with the specifications. Each device shall be tested as a working component of the completed system. All system controls shall be inspected for proper operation and response.

- E. Tests shall demonstrate the response time and display format of each different type of input sensor and output control device. Response time shall be measured with the system functioning at full capacity. Computer operation shall be tested with the complete data file.
- F. The Contractor shall provide a competent trainer who has extensive experience on the installed systems and in delivering training to provide the instruction. As an alternative, the Contractor may propose the use of factory training personnel and coordinate the number of personnel to be trained.

3.3 MAINTENANCE

- A. The Contractor shall offer a Support Agreement (SSA) in order for Technical Support Specialists to reactively troubleshoot system problems.
- B. As part of the agreement, 5x9 telephone support (Standard and Enhanced SSA) will be provided to the Contractor by Certified Technicians. An option of 7x24 Standby telephone support (Enhanced SSA) shall be offered.
- C. As part of the agreement, Flashable and Non-Flashable (Chips) firmware and documentation shall be provided.
- D. As part of the agreement, access to Security Management System (SMS) software patches and software release updates shall be provided.
- E. The Support Agreement shall cover the current version of the SMS software release one full version back, and associated controller hardware.

-----END-----