against entry of foreign matter; and be vacuum cleaned both inside and outside before testing and operating and repainting if required.

2. Damaged equipment shall be, as determined by the Resident Engineer, placed in first class operating condition or be returned to the source of supply for repair or replacement.
3. Painted surfaces shall be protected with factory installed removable heavy craft paper, sheet vinyl or equal.
4. Damaged paint on equipment and materials shall be refinished with the same quality of paint and workmanship as used by the manufacturer so repaired areas are not obvious.

B. Central Station, Workstations, and Controllers:

1. Store in temperature and humidity controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 10 to 30 deg C (50 to 85 deg F), and not more than 80 percent relative humidity, non-condensing.
2. Open each container; verify contents against packing list, and file copy of packing list, complete with container identification for inclusion in operation and maintenance data.
3. Mark packing list with designations which have been assigned to materials and equipment for recording in the system labeling schedules generated by cable and asset management system.
4. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.10 PROJECT CONDITIONS

A. Environmental Conditions: System shall be capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:

1. Interior, Controlled Environment: System components, except central-station control unit, installed in temperature-controlled interior environments shall be rated for continuous operation in ambient conditions of 2 to 50 deg C (36 to 122 deg F) dry bulb and 20 to 90 percent relative humidity, non-condensing. NEMA 250, Type 1 enclosure.
2. Interior, Uncontrolled Environment: System components installed in non-temperature-controlled interior environments shall be rated for continuous operation in ambient conditions of -18 to 50 deg C (0 to 122 deg F) dry bulb and 20 to 90 percent relative humidity, non-condensing. NEMA 250, Type 4X enclosures.
3. Exterior Environment: System components installed in locations exposed to weather shall be rated for continuous operation in ambient

conditions of -34 to 50 deg C (-30 to 122 deg F) dry bulb and 20 to 90 percent relative humidity, condensing. Rate for continuous operation where exposed to rain as specified in NEMA 250, winds up to 137 km/h (85 mph) and snow cover up to 610 mm (24 in) thick. NEMA 250, Type 4X enclosures.

4. Hazardous Environment: System components located in areas where fire or explosion hazards may exist because of flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers shall be rated, listed, and installed according to NFPA 70.
5. Corrosive Environment: For system components subjected to corrosive fumes, vapors, and wind-driven salt spray in coastal zones, provide NEMA 250, Type 4X enclosures.

B. Security Environment: Use vandal resistant enclosures in high-risk areas where equipment may be subject to damage.

C. Console: All console equipment shall, unless noted otherwise, be rated for continuous operation under ambient environmental conditions of 15.6 to 29.4 deg C (60 to 85 deg F) and a relative humidity of 20 to 80 percent.

1.11 EQUIPMENT AND MATERIALS

A. Materials and equipment furnished shall be of current production by manufacturers regularly engaged in the manufacture of such items, for which replacement parts shall be available.

B. When more than one unit of the same class of equipment is required, such units shall be the product of a single manufacturer.

C. Equipment Assemblies and Components:

1. Components of an assembled unit need not be products of the same manufacturer.
2. Manufacturers of equipment assemblies, which include components made by others, shall assume complete responsibility for the final assembled unit.
3. Components shall be compatible with each other and with the total assembly for the intended service.
4. Constituent parts which are similar shall be the product of a single manufacturer.

D. Factory wiring shall be identified on the equipment being furnished and on all wiring diagrams.

E. When Factory Testing Is Specified:

1. The Government shall have the option of witnessing factory tests. The contractor shall notify the VA through the Resident Engineer a

minimum of 15 working days prior to the manufacturers making the factory tests.

2. Four copies of certified test reports containing all test data shall be furnished to the Resident Engineer prior to final inspection and not more than 90 days after completion of the tests.
3. When equipment fails to meet factory test and re-inspection is required, the contractor shall be liable for all additional expenses, including expenses of the Government.

1.12 ELECTRICAL POWER

A. Electrical power of 120 Volts Alternating Current (VAC) shall be indicated on the Division 26 drawings. Additional locations requiring primary power required by the security system shall be shown as part of these contract documents. Primary power for the security system shall be configured to switch to emergency backup sources automatically if interrupted without degradation of any critical system function. Alarms shall not be generated as a result of power switching, however, an indication of power switching on (on-line source) shall be provided to the alarm monitor. The Security Contractor shall provide an interface (dry contact closure) between the PACS and the Uninterruptible Power Supply (UPS) system so the UPS trouble signals and main power fail appear on the PACS operator terminal as alarms.

B. Failure of any on-line battery shall be detected and reported as a fault condition. Battery backed-up power supplies shall be provided sized for 1.5 hours of operation at actual connected load. Requirements for additional power or locations shall be included with the contract to support equipment and systems offered. The following minimum requirements shall be provided for power sources and equipment.

1. Emergency Generator
    a. Report Printers: Unit Control Room
    b. Video Monitors: Unit Control Room
    c. Intercom Stations
    d. Radio System
    e. Lights: Unit Control Room, Equipment Rooms, & Security Offices
    f. Outlets: Security Outlets dedicated to security equipment racks or security enclosure assemblies.
    g. Security Device Power Supplies (DGP, VASS, Card Access, Lock Power, etc.) powered from the security closets or remotely: various locations
    h. Telephone/Radio Recording Equipment: Unit Control Room.
    i. VASS Camera Power Supplies: Security Closets

j. VASS Pan/Tilt Units: Various Locations

k. VASS Outdoor Housing Heaters and Blowers: Various Sites

l. Intercom Master Control System

m. Fiber Optic Receivers/Transmitters

n. Security office Weapons Storage

o. Outlets that charge handheld radios

2. Uninterruptible Power Supply (UPS) on Emergency Power

a. The following 120VAC circuits shall be provided. The Security Contractor shall coordinate exact locations with the Electrical Contractor:

1) Security System Monitors and Keyboards: Control Room and as indicated on the Contract Drawings.

2) CPU: Control Equipment Room and as indicated on the Contract Drawings.

3) Communications equipment: Control Equipment Room and various sites.

4) VASS Network Video Recorder: Control Equipment Room

5) VASS: Control Equipment Room

6) Network Video Recorder, Digital Video Recorders, encoders & decoders: Control Room

7) All equipment Room racked equipment.

8) Network switches

1.13 TRANSIENT VOLTAGE SUPPRESSION, POWER SURGE SUPPLESION, & GROUNDING

A. Transient Voltage Surge Suppression: All cables and conductors extending beyond building façade, except fiber optic cables, which serve as communication, control, or signal lines shall be protected against Transient Voltage surges and have Transient Voltage Surge Suppression (TVSS) protection. The TVSS device shall be UL listed in accordance with Standard TIA 497B installed at each end. Lighting and surge suppression shall be a multi-strike variety and include a fault indicator. Protection shall be furnished at the equipment and additional triple solid state surge protectors rated for the application on each wire line circuit shall be installed within 914.4 mm (3 ft) of the building cable entrance. Fuses shall not be used for surge protection. The inputs and outputs shall be tested in both normal mode and common mode to verify there is no interference.

1. A 10-microsecond rise time by 1000 microsecond pulse width waveform with a peak voltage of 1500 volts and a peak current of 60 amperes.

2. An 8-microsecond rise time by 20-microsecond pulse width waveform with a peak voltage of 1000 volts and a peak current of 500 amperes.

3. Maximum series current: 2 AMPS. Provide units manufactured by Advanced Protection Technologies, model # TE/FA 10B or TE/FA 20B.
4. Operating Temperature and Humidity: -40 to 85 deg C (-40 to 185 deg F), 0 to 95 percent relative humidity.

B. Grounding and Surge Suppression

1. The Security Contractor shall provide grounding and surge suppression to stabilize the voltage under normal operating conditions. To ensure the operation of over current devices, such as fuses, circuit breakers, and relays, underground-fault conditions.
2. Security Contractor shall engineer and provide proper grounding and surge suppression as required by local jurisdiction and prevailing codes and standards referenced in this document.
3. Principal grounding components and features. Include main grounding buses and grounding and bonding connections to service equipment.
4. Details of interconnection with other grounding systems. The lightning protection system shall be provided by the Security Contractor.
5. Locations and sizes of grounding conductors and grounding buses in electrical, data, and communication equipment rooms and closets.
6. AC power receptacles are not to be used as a ground reference point.
7. Any cable that is shielded shall require a ground in accordance with the best practices of the trade and manufactures installation instructions.
8. Protection should be provided at both ends of cabling.

1.14 COMPONENT ENCLOSURES

A. Construction of Enclosures

1. Consoles, power supply enclosures, detector control and terminal cabinets, control units, wiring gutters, and other component housings, collectively referred to as enclosures, shall be so formed and assembled as to be sturdy and rigid.
2. Thickness of metal in-cast and sheet metal enclosures of all types shall not be less than those in Tables I and II, UL 611. Sheet steel used in fabrication of enclosures shall be not less than 14 gauge. Consoles shall be 16-gauge.
3. Doors and covers shall be flanged. Enclosures shall not have pre-punched knockouts. Where doors are mounted on hinges with exposed pins, the hinges shall be of the tight pin type or the ends of hinge pins shall be tack welded to prevent removal. Doors having a latch edge length of less than 609.6 mm (24 in) shall be provided with a single construction core. Where the latch edge of a hinged door is

more than 609.6 mm (24 in) or more in length, the door shall be provided with a three-point latching device with construction core; or alternatively with two, one located near each end.

4. Any ventilator openings in enclosures and cabinets shall conform to the requirements of UL 611. Unless otherwise indicated, sheet metal enclosures shall be designed for wall mounting with tip holes slotted. Mounting holes shall be in positions that remain accessible when all major operating components are in place and the door is open, but shall be in accessible when the door is closed.
5. Covers of pull and junction boxes provided to facilitate initial installation of the system shall be held in place by tamper proof Torx Center post security screws. Stenciled or painted labels shall be affixed to such boxes indicating they contain no connections. These labels shall not indicate the box is part of the Electronic Security System (ESS).

B. Consoles & Equipment Racks: All consoles and vertical equipment racks shall include a forced air-cooling system to be provided by others.
   1. Vertical Equipment Racks:
      a. The forced air blowers shall be installed in the vented top of each cabinet and shall not reduce usable rack space.
      b. The forced air fan shall consist of one fan rated at 105 CFM per rack bay and noise level shall not exceed 55 decibels.
      c. Vertical equipment racks are to be provided with full sized clear plastic locking doors and vented top panels as shown on contract drawings.
   2. Console racks:
      a. Forced air fans shall be installed in the top rear of each console bay. The forced air fan shall consist of one fan rated at 105 CFM mounted to a 133mm vented blank panel the noise level of each fan shall not exceed 55 decibels. The fans shall be installed so air is pulled from the bottom of the rack or cabinet and exhausted out the top.
      b. Console racks are to be provided with flush mounted hinged rear doors with recessed locking latch on the bottom and middle sections of the consoles. Provide code access to support wiring for devices located on the work surfaces.

C. Tamper Provisions and Tamper Switches:
   1. Enclosures, cabinets, housings, boxes and fittings or every product description having hinged doors or removable covers and which contain circuits, or the integrated security system and its power supplies

shall be provided with cover operated, corrosion-resistant tamper switches.

2. Tamper switches shall be arranged to initiate an alarm signal that will report to the monitoring station when the door or cover is moved. Tamper switches shall be mechanically mounted to maximize the defeat time when enclosure covers are opened or removed. It shall take longer than 1 second to depress or defeat the tamper switch after opening or removing the cover. The enclosure and tamper switch shall function together in such a manner as to prohibit direct line of sign to any internal component before the switch activates.
3. Tamper switches shall be inaccessible until the switch is activated. Have mounting hardware concealed so the location of the switch cannot be observed from the exterior of the enclosure. Be connected to circuits which are under electrical supervision at all times, irrespective of the protection mode in which the circuit is operating. Be spring-loaded and held in the closed position by the door or cover and be wired so they break the circuit when the door cover is disturbed. Tamper circuits shall be adjustable type screw sets and shall be adjusted by the contractor to eliminate nuisance alarms associated with incorrectly mounted tamper device shall annunciate prior to the enclosure door opening (within 1/4 " tolerance. The tamper device or its components shall not be visible or accessing with common tools to bypass when the enclosure is in the secured mode.
4. The single gang junction boxes for the portrait alarming and pull boxes with less than 102 square mm will not require tamper switches.
5. All enclosures over 305 square mm shall be hinged with an enclosure lock.
6. Control Enclosures: Maintenance/Safety switches on control enclosures, which must be opened to make routing maintenance adjustments to the system and to service the power supplies, shall be push/pull-set automatic reset type.
7. Provide one (1) enclosure tamper switch for each 609 linear mm of enclosure lock side opening evenly spaced.
8. All security screws shall be Torx-Post Security Screws.
9. The contractor shall provide the owner with two (2) torx-post screwdrivers.

1.15 ELECTRONIC COMPONENTS

A. All electronic components of the system shall be of the solid-state type, mounted on printed circuit boards conforming to UL 796. Boards shall be plug-in, quick-disconnect type. Circuitry shall not be so densely placed as to impede maintenance. All power-dissipating components shall incorporate safety margins of not less than 25 percent with respect to dissipation ratings, maximum voltages, and current-carrying capacity.

1.16 SUBSTITUTE MATERIALS & EQUIPMENT

A. Where variations from the contract requirements are requested in accordance with the GENERAL CONDITIONS and Section 01 33 23, SHOP DRAWINGS, PRODUCT DATA, AND SAMPLES, the connecting work and related components shall include, but not be limited to additions or changes to branch circuits, circuit protective devices, conduits, wire, feeders, controls, panels and installation methods.

B. In addition to this Section the Security Contractor shall also reference Section II, Products and associated divisions. The Resident Engineer shall have final authority on the authorization or refusal of substitutions. If there are no proposed substitutions, a statement in writing from the Contractor shall be submitted to the Resident Engineer stating same. In the preparation of a list of substitutions, the following information shall be included, as a minimum:

1. Identity of the material or devices specified for which there is a proposed substitution.
2. Description of the segment of the specification where the material or devices are referenced.
3. Identity of the proposed substitute by manufacturer, brand name, catalog or model number and the manufacturer’s product name.
4. A technical statement of all operational characteristic expressing equivalence to items to be substituted and comparison, feature-by-feature, between specification requirements and the material or devices called for in the specification; and Price differential.

C. Materials Not Listed: Furnish all necessary hardware, software, programming materials, and supporting equipment required to place the specified major subsystems in full operation. Note that some supporting equipment, materials, and hardware may not be described herein. Depending on the manufacturers selected by the COTR, some equipment, materials and hardware may not be contained in either the Contract Documents or these written specifications, but are required by the manufacturer for complete operation according to the intent of the design and these specifications. In such cases, the Resident Engineer shall be given the opportunity to approve the additional equipment, hardware and materials that shall be fully identified in the bid and in the equipment list submittal. The Resident Engineer shall be consulted in the event there is any question about which supporting equipment, materials, or hardware is intended to be included.

D. Response to Specification: The Contractor shall submit a point-by-point statement of compliance with each paragraph of the security specification. The statement of compliance shall list each paragraph by number and indicate “COMPLY” opposite the number for each paragraph where the Contractor fully complies with the specification. Where the proposed system cannot meet the requirements of the paragraph, and does not offer an equivalent solution, the offers shall indicate “DOES NOT COMPLY” opposite the paragraph number. Where the proposed system does not comply with the paragraph as written, but the bidder feels it will accomplish the intent of the paragraph in a manner different from that described, the offers shall indicate “COMPARABLE”. The offers shall include a statement fully describing the “comparable” method of satisfying the requirement. Where a full and concise description is not provided, the offered system shall be considered as not complying with the specification. Any submission that does not include a point-by-point statement of compliance, as described above, shall be disqualified. Submittals for products shall be in precise order with the product section of the specification. Submittals not in proper sequence will be rejected.

1.17 LIKE ITEMS

A. Where two or more items of equipment performing the same function are required, they shall be exact duplicates produced by one manufacturer. All equipment provided shall be complete, new, and free of any defects.

1.18 WARRANTY

A. The Contractor shall, as a condition precedent to the final payment, execute a written guarantee (warranty) to the COTR certifying all contract requirements have been completed according to the final specifications. Contract drawings and the warranty of all materials and equipment furnished under this contract are to remain in satisfactory operating condition (ordinary wear and tear, abuse and causes beyond his control for this work accepted) for one (1) year from the date the Contactor received written notification of final acceptance from the COTR. Demonstration and training shall be performed prior to system acceptance. All defects or damages due to faulty materials or workmanship shall be repaired or replaced without delay, to the COTR's satisfaction, and at the Contractor's expense. The Contractor shall provide quarterly inspections during the warranty period. The contractor shall provide written documentation to the COTR on conditions and findings of the system and device(s). In addition, the contractor shall provide written documentation of test results and stating what was done to correct any deficiencies. The first inspection shall occur 90 calendar days after the acceptance date. The last inspection shall occur 30 calendar days prior to the end of the warranty. The warranty period shall be extended until the last inspection and associated corrective actions are complete. When equipment and labor covered by the Contractor's warranty, or by a manufacturer's warranty, have been replaced or restored because of its failure during the warranty period, the warranty period for the replaced or repaired equipment or restored work shall be reinstated for a period equal to the original warranty period, and commencing with the date of completion of the replacement or restoration work. In the event any manufacturer customarily provides a warranty period greater than one (1) year, the Contractor's warranty shall be for the same duration for that component.

1.19 SINGULAR NUMBER

Where any device or part of equipment is referred to in these specifications in the singular number (e.g., "the switch"), this reference shall be deemed to apply to as many such devices as are required to complete the installation as shown on the drawings.

PART 2 – PRODUCTS – NOT USED

PART 3 – EXECUTION – NOT USED

- - - E N D - - -

SECTION 28 05 13
CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY

PART 1 - GENERAL

1.1 DESCRIPTION

A. This section specifies the finishing, installation, connection, testing and certification the conductors and cables required for a fully functional for electronic safety and security (ESS) system.

1.2 RELATED WORK

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.

C. 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.

D. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for personnel safety and to provide a low impedance path for possible ground fault currents.

E. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SECURITY AND SAFETY. Requirements for infrastructure.

F. Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS. Requirements for commissioning.

G. Section 31 20 00 - EARTH MOVING. For excavation and backfill for cables that are installed in conduit.

1.3 DEFINITIONS

A. BICSI: Building Industry Consulting Service International.

B. EMI: Electromagnetic interference.

C. IDC: Insulation displacement connector.

D. Ladder Cable Tray: A fabricated structure consisting of two longitudinal side rails connected by individual transverse members (rungs).

E. Low Voltage: As defined in NFPA 70 for circuits and equipment operating at less than 50 V or for remote-control and signaling power-limited circuits.

F. Open Cabling: Passing telecommunications cabling through open space (e.g., between the studs of a wall cavity).

G. RCDD: Registered Communications Distribution Designer.

H. Solid-Bottom or Nonventilated Cable Tray: A fabricated structure consisting of integral or separate longitudinal side rails, and a bottom without ventilation openings.

I. Trough or Ventilated Cable Tray: A fabricated structure consisting of integral or separate longitudinal rails and a bottom having openings sufficient for the passage of air and using 75 percent or less of the plan area of the surface to support cables.

J. UTP: Unshielded twisted pair.

1.4 QUALITY ASSURANCE

A. See section 28 05 00, Paragraph 1.4.

1.5 SUBMITTALS

A. In accordance with Section 01 33 23, SHOP DRAWINGS, PRODUCT DATA, AND SAMPLES, furnish the following:

1. Manufacturer's Literature and Data: Showing each cable type and rating.
2. Certificates: Two weeks prior to final inspection, deliver to the Resident Engineer/COTR four copies of the certification that the material is in accordance with the drawings and specifications and diagrams for cable management system.
3. Shop Drawings: Cable tray layout, showing cable tray route to scale, with relationship between the tray and adjacent structural, electrical, and mechanical elements. Include the following:
    a. Vertical and horizontal offsets and transitions.
    b. Clearances for access above and to side of cable trays.
    c. Vertical elevation of cable trays above the floor or bottom of ceiling structure.
    d. Load calculations to show dead and live loads as not exceeding manufacturer's rating for tray and its support elements.
    e. System labeling schedules, including electronic copy of labeling schedules that are part of the cable and asset identification system of the software specified in Parts 2 and 3.
4. Wiring Diagrams. Show typical wiring schematics including the following:
    a. Workstation outlets, jacks, and jack assemblies.
    b. Patch cords.
    c. Patch panels.
5. Cable Administration Drawings: As specified in Part 3 "Identification" Article.
6. Project planning documents as specified in Part 3.
7. Maintenance Data: For wire and cable to include in maintenance manuals.

1.6 APPLICABLE PUBLICATIONS

A. Publications listed below (including amendments, addenda, revisions, supplements and errata) form a part of this specification to the extent referenced. Publications are reference in the text by the basic designation only.

B. American Society of Testing Material (ASTM):

D2301-04................Standard Specification for Vinyl Chloride Plastic Pressure Sensitive Electrical Insulating Tape

C. Federal Specifications (Fed. Spec.):

A-A-59544-08...........Cable and Wire, Electrical (Power, Fixed Installation)

D. National Fire Protection Association (NFPA):

70-11...................National Electrical Code (NEC)

E. Underwriters Laboratories, Inc. (UL):

44-05...................Thermoset-Insulated Wires and Cables

83-08...................Thermoplastic-Insulated Wires and Cables

467-07..................Electrical Grounding and Bonding Equipment

486A-03.................Wire Connectors and Soldering Lugs for Use with Copper Conductors

486C-04.................Splicing Wire Connectors

486D-05.................Insulated Wire Connector Systems for Underground Use or in Damp or Wet Locations

486E-00.................Equipment Wiring Terminals for Use with Aluminum and/or Copper Conductors

493-07..................Thermoplastic-Insulated Underground Feeder and Branch Circuit Cable

514B-04.................Fittings for Cable and Conduit

1479-03.................Fire Tests of Through-Penetration Fire Stops//

1.7 DELIVERY, STORAGE, AND HANDLING

A. Test cables upon receipt at Project site.

1. Test optical fiber cable to determine the continuity of the strand end to end. Use optical loss test set.
2. Test optical fiber cable on reels. Use an optical time domain reflectometer to verify the cable length and locate cable defects, splices, and connector; include the loss value of each. Retain test data and include the record in maintenance data.
3. Test each pair of UTP cable for open and short circuits.

1.8 PROJECT CONDITIONS

A. Environmental Limitations: Do not deliver or install UTP, optical fiber, and coaxial cables and connecting materials until wet work in spaces is complete and dry, and temporary HVAC system is operating and maintaining ambient temperature and humidity conditions at occupancy levels during the remainder of the construction period.

PART 2 - PRODUCTS

2.1 GENERAL

A. General: All cabling locations for the PACS System shall be in conduit systems as outlined in Division 28 unless a waiver is granted in writing or an exception is noted on the construction drawings. All cabling locations for the CCTV System shall be in conduit except where otherwise shown on the Contract Drawings.

B. Conduit and Boxes: Comply with requirements in Division 28 Section "Conduits and Backboxes for Electrical Systems. Flexible metal conduit shall not be used.

1. Outlet boxes shall be no smaller than 2 inches wide, 3 inches high, and 2-1/2 inches deep.

2.2 BACKBOARDS

A. Backboards: Plywood, fire-retardant treated, 3/4 by 48 by 96. Comply with requirements for plywood backing panels in Division 06 Section "Rough Carpentry".

2.3 UTP CABLE

A. Description: 100-ohm, 4-pair UTP, formed into 25-pair binder groups covered with a blue thermoplastic jacket.

1. Comply with ICEA S-90-661 for mechanical properties.
2. Comply with TIA/EIA-568-B.1 for performance specifications.
3. Comply with TIA/EIA-568-B.2, Category 6.
4. Listed and labeled by an NRTL acceptable to authorities having jurisdiction as complying with UL 444 and NFPA 70 for the following types:
   a. Communications, Plenum Rated: Type CMP, complying with NFPA 262.
   b. Multipurpose, Plenum Rated: Type MPP, complying with NFPA 262.

2.4 UTP CABLE HARDWARE

A. UTP Cable Connecting Hardware: IDC type, using modules designed for punch-down caps or tools. Cables shall be terminated with connecting hardware of the same category or higher.

B. Connecting Blocks: 110-style for Category 6. Provide blocks for the number of cables terminated on the block, plus 25 percent spare.

Integral with connector bodies, including plugs and jacks where indicated.

2.5 OPTICAL FIBER CABLE

A. Description: Single-mode, 8.3/125-micrometer, 12-fiber, loose tube, optical fiber cable.

1. Comply with ICEA S-83-596 for mechanical properties.
2. Comply with TIA/EIA-568-B.3 for performance specifications.
3. Comply with TIA/EIA-492AAAA-B for detailed specifications.
4. Listed and labeled by an NRTL acceptable to authorities having jurisdiction as complying with UL 444, UL 1651, and NFPA 70 for the following types:
   a. Plenum Rated, Nonconductive: Type OFNP, complying with NFPA 262.
   b. Plenum Rated, Conductive: Type OFCP or OFNP, complying with NFPA 262.
5. Conductive cable shall be steel armored type.

B. Jacket:

1. Jacket Color: As selected by VA IT personnel from industry standard jacket color selection.
2. Cable cordage jacket, fiber, unit, and group color shall be according to TIA/EIA-598-B.
3. Imprinted with fiber count, fiber type, and aggregate length at regular intervals not to exceed 40 inches.

2.6 OPTICAL FIBER CABLE HARDWARE

A. Cable Connecting Hardware: Meet the Optical Fiber Connector Intermateability Standards (FOCIS) specifications of TIA/EIA-604-2, TIA/EIA-604-3-A, and TIA/EIA-604-12. Comply with TIA/EIA-568-B.3.

1. Quick-connect, simplex and duplex, coordinate exact type of connectors required with hospital and equipment supplier. Insertion loss shall be not more than 0.75 dB.
2. Type SC connectors shall be used in termination racks, panels, and equipment packages.

2.7 COAXIAL CABLE

A. General Coaxial Cable Requirements: CCTV type, recommended by cable manufacturer specifically for security video transmission applications. Coaxial cable and accessories shall have 75-ohm nominal impedance with a return loss of 20 dB maximum from 1 MHz to 1 GHz. Refer to Division 28 Specification Section "Video Surveillance" for coaxial cable type for cameras.

B. RG-11/U: NFPA 70, Type CATV.

1. No. 14 AWG, solid, copper conductor.

2. Gas-injected, foam-PE insulation.
3. Bare copper braid with 95 percent coverage.
4. Jacketed with sunlight-resistant, black PVC or PE.
5. Suitable for outdoor installations in ambient temperatures ranging from minus 40 to plus 85 deg C.

C. RG-6/U: NFPA 70, Type CM or CMP.

1. No. 16 AWG, solid, copper conductor; gas-injected, foam-PE insulation.
2. Bare copper braid with 95 percent coverage.
3. Jacketed with black PVC or PE.
4. Suitable for indoor installations.

D. NFPA and UL compliance, listed and labeled by an NRTL acceptable to authorities having jurisdiction as complying with UL

2.8 COAXIAL CABLE HARDWARE

A. Coaxial-Cable Connectors: Type BNC, 75 ohms.

2.9 RS-232 CABLE

A. Plenum-Rated Cable: NFPA 70, Type CMP.

1. Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors.
2. Plastic insulation.
3. Individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage.
4. Plastic jacket.
5. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
6. Flame Resistance: Comply with NFPA 262.

2.10 RS-485 CABLE

A. Plenum-Rated Cable: NFPA 70, Type CMP.

1. Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors.
2. Fluorinated ethylene propylene insulation.
3. Unshielded.
4. Fluorinated ethylene propylene jacket.
5. Flame Resistance: NFPA 262, Flame Test.

2.11 LOW-VOLTAGE CONTROL CABLE

A. Plenum-Rated, Paired Lock Cable: NFPA 70, Type CMP.

1. 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors.
2. PVC insulation.
3. Unshielded.

4. PVC jacket.
5. Flame Resistance: Comply with NFPA 262.

B. Plenum-Rated, Paired Lock Cable: NFPA 70, Type CMP.

1. 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors.
2. Fluorinated ethylene propylene insulation.
3. Unshielded.
4. Plastic jacket.
5. Flame Resistance: NFPA 262, Flame Test.

2.12 CONTROL-CIRCUIT CONDUCTORS

A. Class 1 Control Circuits: Stranded copper, Type THHN-THWN, in raceway complying with UL 83.

B. Class 2 Control Circuits: Stranded copper, Type THHN-THWN, in raceway complying with UL 83.

C. Class 3 Remote-Control and Signal Circuits: Stranded copper, Type TW or TF, complying with UL 83.

2.13 IDENTIFICATION PRODUCTS

A. Comply with UL 969 for a system of labeling materials, including label stocks, laminating adhesives, and inks used by label printers.

2.14 SOURCE QUALITY CONTROL

A. Testing Agency: Engage a qualified testing agency to evaluate cables.

B. Factory test UTP and optical fiber cables on reels according to TIA/EIA-568-B.1.

C. Factory test UTP cables according to TIA/EIA-568-B.2.

D. Factory test multimode optical fiber cables according to TIA/EIA-526-14-A and TIA/EIA-568-B.3.

E. Factory sweep test coaxial cables at frequencies from 5 MHz to 1 GHz. Sweep test shall test the frequency response, or attenuation over frequency, of a cable by generating a voltage whose frequency is varied through the specified frequency range and graphing the results.

F. Cable will be considered defective if it does not pass tests and inspections.

G. Prepare test and inspection reports.

2.15 WIRE LUBRICATING COMPOUND

A. Suitable for the wire insulation and conduit it is used with, and shall not harden or become adhesive.

B. Shall not be used on wire for isolated type electrical power systems.

2.16 FIREPROOFING TAPE

A. The tape shall consist of a flexible, conformable fabric of organic composition coated one side with flame-retardant elastomer.

B. The tape shall be self-extinguishing and shall not support combustion. It shall be arc-proof and fireproof.

C. The tape shall not deteriorate when subjected to water, gases, salt water, sewage, or fungus and be resistant to sunlight and ultraviolet light.

D. The finished application shall withstand a 200-ampere arc for not less than 30 seconds.

E. Securing tape: Glass cloth electrical tape not less than 7 mils thick, and 3/4 inch wide.

PART 3 - EXECUTION

3.1 INSTALLATION OF CONDUCTORS AND CABLES

A. Comply with NECA 1.

B. General Requirements for Cabling:

1. Comply with TIA/EIA-568-B.1.
2. Comply with BICSI ITSIM, Ch. 6, "Cable Termination Practices."
3. Install 110-style IDC termination hardware unless otherwise indicated.
4. Terminate all conductors; no cable shall contain un-terminated elements. Make terminations only at indicated outlets, terminals, and cross-connect and patch panels.
5. Cables may not be spliced. Secure and support cables at intervals not exceeding 30 inches and not more than 6 inches from cabinets, boxes, fittings, outlets, racks, frames, and terminals.
6. Bundle, lace, and train conductors to terminal points without exceeding manufacturer's limitations on bending radii, but not less than radii specified in BICSI ITSIM, "Cabling Termination Practices" Chapter. Install lacing bars and distribution spools.
7. Do not install bruised, kinked, scored, deformed, or abraded cable. Do not splice cable between termination, tap, or junction points. Remove and discard cable if damaged during installation and replace it with new cable.
8. Cold-Weather Installation: Bring cable to room temperature before dereeling. Heat lamps shall not be used for heating.
9. Pulling Cable:
   a. Comply with BICSI ITSIM, Ch. 4, "Pulling Cable." Monitor cable pull tensions.

b. Provide installation equipment that will prevent the cutting or abrasion of insulation during pulling of cables.

c. Use ropes made of nonmetallic material for pulling feeders.

d. Attach pulling lines for feeders by means of either woven basket grips or pulling eyes attached directly to the conductors, as approved by the COTR.

e. Pull in multiple cables together in a single conduit.

C. Splice cables and wires where necessary only in outlet boxes, junction boxes, or pull boxes.

1. Splices and terminations shall be mechanically and electrically secure.
2. Where the Government determines that unsatisfactory splices or terminations have been installed, remove the devices and install approved devices at no additional cost to the Government.

D. Seal cable and wire entering a building from underground, between the wire and conduit where the cable exits the conduit, with a non-hardening approved compound.

E. Unless otherwise specified in other sections install wiring and connect to equipment/devices to perform the required functions as shown and specified.

F. Except where otherwise required, install a separate power supply circuit for each system so that malfunctions in any system will not affect other systems.

G. Where separate power supply circuits are not shown, connect the systems to the nearest panel boards of suitable voltages, which are intended to supply such systems and have suitable spare circuit breakers or space for installation.

H. Install a red warning indicator on the handle of the branch circuit breaker for the power supply circuit for each system to prevent accidental de-energizing of the systems.

I. System voltages shall be 120 volts or lower where shown on the drawings or as required by the NEC.

J. UTP Cable Installation:

1. Comply with TIA/EIA-568-B.2.
2. Do not untwist UTP cables more than 1/2 inch (12 mm) from the point of termination to maintain cable geometry.

K. Optical Fiber Cable Installation:

1. Comply with TIA/EIA-568-B.3.
2. Cable shall be terminated on connecting hardware that is rack or cabinet mounted.

L. Outdoor Coaxial Cable Installation:

1. Install outdoor connections in enclosures complying with NEMA 250, Type 4X. Install corrosion-resistant connectors with properly designed O-rings to keep out moisture.

M. Separation from EMI Sources:

1. Comply with BICSI TDMM and TIA/EIA-569-A recommendations for separating unshielded copper voice and data communication cable from potential EMI sources, including electrical power lines and equipment.
2. Separation between open communications cables or cables in nonmetallic raceways and unshielded power conductors and electrical equipment shall be as follows:
   a. Electrical Equipment Rating Less Than 2 kVA: A minimum of 5 inches.
   b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 12 inches.
   c. Electrical Equipment Rating More Than 5 kVA: A minimum of 24 inches.
3. Separation between communications cables in grounded metallic raceways and unshielded power lines or electrical equipment shall be as follows:
   a. Electrical Equipment Rating Less Than 2 kVA: A minimum of 2-1/2 inches.
   b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 6 inches.
   c. Electrical Equipment Rating More Than 5 kVA: A minimum of 12 inches.
4. Separation between communications cables in grounded metallic raceways and power lines and electrical equipment located in grounded metallic conduits or enclosures shall be as follows:
   a. Electrical Equipment Rating Less Than 2 kVA: No requirement.
   b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 3 inches.
   c. Electrical Equipment Rating More Than 5 kVA: A minimum of 6 inches.
5. Separation between Cables and Electrical Motors and Transformers, 5 kVA or HP and Larger: A minimum of 48 inches.
6. Separation between Cables and Fluorescent Fixtures: A minimum of 5 inches.

3.2 CONTROL CIRCUIT CONDUCTORS

A. Minimum Conductor Sizes:

1. Class 1 remote-control and signal circuits, No. 14 AWG.
2. Class 2 low-energy, remote-control and signal circuits, No. 16 AWG.
3. Class 3 low-energy, remote-control, alarm and signal circuits, No. 12 AWG.

3.3 CONNECTIONS

A. Comply with requirements in Division 28 Section, PHYSICAL ACCESS CONTROL for connecting, terminating, and identifying wires and cables.

B. Comply with requirements in Division 28 Section "VIDEO SURVEILLANCE" for connecting, terminating, and identifying wires and cables.

3.4 FIRESTOPPING

A. Comply with requirements in Division 07 Section "PENETRATION FIRESTOPPING" and the Contract Drawings.

B. Comply with TIA/EIA-569-A, "Firestopping" Annex A.

C. Comply with BICSI TDMM, "Firestopping Systems" Article.

3.5 GROUNDING

A. For communications wiring, comply with ANSI-J-STD-607-A and with BICSI TDMM, "Grounding, Bonding, and Electrical Protection" Chapter.

B. For low-voltage wiring and cabling, comply with requirements in Division 28 Section "GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY."

3.6 IDENTIFICATION

A. Identify system components, wiring, and cabling complying with TIA/EIA-606-A.

B. Install a permanent wire marker on each wire at each termination.

C. Identifying numbers and letters on the wire markers shall correspond to those on the wiring diagrams used for installing the systems.

D. Wire markers shall retain their markings after cleaning.

E. In each handhole, install embossed brass tags to identify the system served and function.

3.7 FIELD QUALITY CONTROL

A. Testing Agency: Engage a qualified testing agency to perform tests and inspections.

B. Perform tests and inspections.

C. Tests and Inspections:

1. Visually inspect UTP and optical fiber cable jacket materials for UL or third-party certification markings. Inspect cabling terminations to confirm color-coding for pin assignments, and inspect cabling connections to confirm compliance with TIA/EIA-568-B.1.

2. Visually inspect cable placement, cable termination, grounding and bonding, equipment and patch cords, and labeling of all components.
3. Test UTP cabling for DC loop resistance, shorts, opens, intermittent faults, and polarity between conductors. Test operation of shorting bars in connection blocks. Test cables after termination but not cross connection.
   a. Test instruments shall meet or exceed applicable requirements in TIA/EIA-568-B.2. Perform tests with a tester that complies with performance requirements in "Test Instruments (Normative)" Annex, complying with measurement accuracy specified in "Measurement Accuracy (Informative)" Annex. Use only test cords and adapters that are qualified by test equipment manufacturer for channel or link test configuration.
4. Optical Fiber Cable Tests:
   a. Test instruments shall meet or exceed applicable requirements in TIA/EIA-568-B.1. Use only test cords and adapters that are qualified by test equipment manufacturer for channel or link test configuration.
   b. Link End-to-End Attenuation Tests:
      1) Multimode Link Measurements: Test at 850 or 1300 nm in 1 direction according to TIA/EIA-526-14-A, Method B, One Reference Jumper.
      2) Attenuation test results for links shall be less than 2.0 dB. Attenuation test results shall be less than that calculated according to equation in TIA/EIA-568-B.1.

D. Document data for each measurement. Print data for submittals in a summary report that is formatted using Table 10.1 in BICSI TDMM as a guide, or transfer the data from the instrument to the computer, save as text files, print, and submit.

E. End-to-end cabling will be considered defective if it does not pass tests and inspections.

F. Prepare test and inspection reports.

3.8 EXISTING WIRING

A. Unless specifically indicated on the plans, existing wiring shall not be reused for the new installation. Only wiring that conforms to the specifications and applicable codes may be reused. If existing wiring does not meet these requirements, existing wiring may not be reused and new wires shall be installed.

- - - E N D - - -

SECTION 28 05 26
GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY

PART 1 - GENERAL

1.1 DESCRIPTION

A. This section specifies the finishing, installation, connection, testing and certification of the grounding and bonding required for a fully functional Electronic Safety and Security (ESS) system.

B. “Grounding electrode system” refers to all electrodes required by NEC, as well as including made, supplementary, grounding electrodes.

C. The terms “connect” and “bond” are used interchangeably in this specification and have the same meaning

1.2 RELATED WORK

A. Section 28 05 00 - REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY INSTALLATIONS. For general electrical requirements, quality assurance, coordination, and project conditions that are common to more than one section in Division 28.

B. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for low voltage power and lighting wiring.

C. Section 28 08 00 - COMMISIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS. Requirements for commissioning.

1.3 SUBMITTALS

A. Submit in accordance with Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

B. Shop Drawings:

1. Clearly present enough information to determine compliance with drawings and specifications.
2. Include the location of system grounding electrode connections and the routing of aboveground and underground grounding electrode conductors.

C. Test Reports: Provide certified test reports of ground resistance.

D. Certifications: Two weeks prior to final inspection, submit four copies of the following to the COTR:

1. Certification that the materials and installation are in accordance with the drawings and specifications.
2. Certification by the contractor that the complete installation has been properly installed and tested.

1.4 APPLICABLE PUBLICATIONS

A. Publications listed below (including amendments, addenda, revisions, supplements, and errata) form a part of this specification to the extent referenced. Publications are referenced in the text by designation only.

B. American Society for Testing and Materials (ASTM):

B1-07	Standard Specification for Hard-Drawn Copper Wire
B3-07	Standard Specification for Soft or Annealed Copper Wire
B8-04	Standard Specification for Concentric-Lay-Stranded Copper Conductors, Hard, Medium-Hard, or Soft

C. Institute of Electrical and Electronics Engineers, Inc. (IEEE):

81-1983	IEEE Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System
C2-07	National Electrical Safety Code

D. National Fire Protection Association (NFPA):

70-11	National Electrical Code (NEC)
99-2005	Health Care Facilities

E. Underwriters Laboratories, Inc. (UL):

44-05	Thermoset-Insulated Wires and Cables
83-08	Thermoplastic-Insulated Wires and Cables
467-07	Grounding and Bonding Equipment
486A-486B-03	Wire Connectors

PART 2 - PRODUCTS

2.1 GROUNDING AND BONDING CONDUCTORS

A. Equipment grounding conductors shall be UL 83 insulated stranded copper, except that sizes 10 AWG and smaller shall be solid copper. Insulation color shall be continuous green for all equipment grounding conductors, except that wire sizes 4 AWG and larger shall be permitted to be identified per NEC.

B. Bonding conductors shall be ASTM B8 bare stranded copper, except that sizes 10 AWG and smaller shall be ASTM B1 solid bare copper wire.

2.2 SPLICES AND TERMINATION COMPONENTS

A. Components shall meet or exceed UL 467 and be clearly marked with the manufacturer, catalog number, and permitted conductor size(s) ground connections

B. Listed and labeled by an NRTL acceptable to authorities having jurisdiction for applications in which used and for specific types, sizes, and combinations of conductors and other items connected.

C. Below Grade: Exothermic-welded type connectors.

D. Above Grade:

1. Bonding Jumpers: Compression-type connectors, using zinc-plated fasteners and external tooth lockwashers.
2. Connection to Building Steel: Exothermic-welded type connectors.
3. Ground Busbars: Two-hole compression type lugs, using tin-plated copper or copper alloy bolts and nuts.
4. Rack and Cabinet Ground Bars: One-hole compression-type lugs, using zinc-plated or copper alloy fasteners.
5. Bolted Connectors for Conductors and Pipes: Copper or copper alloy, pressure type with at least two bolts.
   a) Pipe Connectors: Clamp type, sized for pipe.
6. Welded Connectors: Exothermic-welding kits of types recommended by kit manufacturer for materials being joined and installation conditions.

2.3 EQUIPMENT RACK GROUND BARS

A. Provide solid copper ground bars designed for mounting on the framework of open or cabinet-enclosed equipment racks with minimum dimensions of 3/8 inch x 3/4 inch.

2.4 GROUND TERMINAL BLOCKS

A. At any equipment mounting location (e.g., backboards and hinged cover enclosures) where rack-type ground bars cannot be mounted, provide screw lug-type terminal blocks.

2.5 SPLICE CASE GROUND ACCESSORIES

A. Splice case grounding and bonding accessories shall be supplied by the splice case manufacturer when available. Otherwise, use 16 mm^2 (6 AWG) insulated ground wire with shield bonding connectors.

PART 3 - EXECUTION

3.1 GENERAL

A. Ground in accordance with the NEC, as shown on drawings, and as specified herein.

B. Equipment Grounding: Metallic structures, including ductwork and building steel, enclosures, raceways, junction boxes, outlet boxes, cabinets, machine frames, and other conductive items in close proximity with electrical circuits, shall be bonded and grounded.

3.2 INACCESSIBLE GROUNDING CONNECTIONS

A. Make grounding connections, which are buried or otherwise normally inaccessible (except connections for which periodic testing access is required) by exothermic weld.

3.3 CORROSION INHIBITORS

A. When making ground and ground bonding connections, apply a corrosion inhibitor to all contact surfaces. Use corrosion inhibitor appropriate for protecting a connection between the metals used.

3.4 EXTERIOR LIGHT/CAMERA POLES

A. Provide 20 ft [6.1 M] of No. 4 bare copper coiled at bottom of pole base excavation prior to pour, plus additional unspliced length in and above foundation as required to reach pole ground stud.

3.5 GROUNDING FOR RF/EMI CONTROL

A. Install bonding jumpers to bond all conduit, cable trays, sleeves and equipment for low voltage signaling and data communications circuits. Bonding jumpers shall consist of 4 inches wide copper strip or two 10 AWG copper conductors spaced minimum 100 mm 4 inches apart. Use 6 AWG copper where exposed and subject to damage.

B. Comply with the following when shielded cable is used for data circuits.

1. Shields shall be continuous throughout each circuit.
2. Connect shield drain wires together at each circuit connection point and insulate from ground. Do not ground the shield.
3. Do not connect shields from different circuits together.
4. Shield shall be connected at one end only. Connect shield to signal reference at the origin of the circuit. Consult with equipment manufacturer to determine signal reference.

3.6 LABELING

A. Comply with requirements in Division 26 Section "ELECTRICAL IDENTIFICATION" Article for instruction signs. The label or its text shall be green.

B. Install labels at the telecommunications bonding conductor and grounding equalizer and at the grounding electrode conductor where exposed

1. Label Text: "If this connector or cable is loose or if it must be removed for any reason, notify the facility manager."

3.7 FIELD QUALITY CONTROL

A. Perform tests and inspections.

B. Tests and Inspections:

1. After installing grounding system but before permanent electrical circuits have been energized, test for compliance with requirements.
2. Inspect physical and mechanical condition. Verify tightness of accessible, bolted, electrical connections with a calibrated torque wrench according to manufacturer's written instructions.

C. Grounding system will be considered defective if it does not pass tests and inspections.

D. Prepare test and inspection reports.

- - - END - - -

SECTION 28 08 00
COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS

PART 1 - GENERAL

1.1 DESCRIPTION

A. The requirements of this Section apply to all sections of Division 28.

B. This project will have selected building systems commissioned. The complete list of equipment and systems to be commissioned are specified in Section 01 91 00 GENERAL COMMISSIONING REQUIREMENTS. The commissioning process, which the Contractor is responsible to execute, is defined in Section 01 91 00 GENERAL COMMISSIONING REQUIREMENTS. A Commissioning Agent (CxA) appointed by the VA will manage the commissioning process.

1.2 RELATED WORK

A. Section 01 00 00 GENERAL REQUIREMENTS.

B. Section 01 33 23 SHOP DRAWINGS, PRODUCT DATA, AND SAMPLES.

1.3 SUMMARY

A. This Section includes requirements for commissioning the electronic safety and security systems, subsystems and equipment. This Section supplements the general requirements specified in Section 01 91 00 GENERAL COMMISSIONING REQUIREMENTS.

B. The commissioning activities have been developed to support the VA requirements to meet guidelines for Federal Leadership in Environmental, Energy, and Economic Performance.

C. Refer to Section 01 91 00 GENERAL COMMISSIONING REQUIREMENTS for more specifics regarding processes and procedures as well as roles and responsibilities for all Commissioning Team members.

1.4 DEFINITIONS

A. Refer to Section 01 91 00 GENERAL COMMISSIONING REQUIREMENTS for definitions.

1.5 COMMISSIONED SYSTEMS

A. Commissioning of a system or systems specified in this Division is part of the construction process. Documentation and testing of these systems, as well as training of the VA’s Operation and Maintenance personnel, is required in cooperation with the VA and the Commissioning Agent.

B. The following Electronic Safety and Security systems will be commissioned:

1. PACS System.
2. CCTV System.

1.6 SUBMITTALS

A. The commissioning process requires review of selected Submittals. The Commissioning Agent will provide a list of submittals that will be reviewed by the Commissioning Agent. This list will be reviewed and approved by the Resident Engineer prior to forwarding to the Contractor. Refer to Section 01 33 23 SHOP DRAWINGS, PRODUCT DATA, and SAMPLES for further details.

B. The commissioning process requires Submittal review simultaneously with engineering review. Specific submittal requirements related to the commissioning process are specified in Section 01 91 00 GENERAL COMMISSIONING REQUIREMENTS.

PART 2 - PRODUCTS (NOT USED)

PART 3 - EXECUTION

3.1 PRE-FUNCTIONAL CHECKLISTS

A. The Contractor shall complete Pre-Functional Checklists to verify systems, subsystems, and equipment installation is complete and systems are ready for Systems Functional Performance Testing. The Commissioning Agent will prepare Pre-Functional Checklists to be used to document equipment installation. The Contractor shall complete the checklists. Completed checklists shall be submitted to the VA and to the Commissioning Agent for review. The Commissioning Agent may spot check a sample of completed checklists. If the Commissioning Agent determines that the information provided on the checklist is not accurate, the Commissioning Agent will return the marked-up checklist to the Contractor for correction and resubmission. If the Commissioning Agent determines that a significant number of completed checklists for similar equipment are not accurate, the Commissioning Agent will select a broader sample of checklists for review. If the Commissioning Agent determines that a significant number of the broader sample of checklists is also inaccurate, all the checklists for the type of equipment will be returned to the Contractor for correction and resubmission. Refer to SECTION 01 91 00 GENERAL COMMISSIONING

REQUIREMENTS for submittal requirements for Pre-Functional Checklists, Equipment Startup Reports, and other commissioning documents.

3.2 CONTRACTORS TESTS

A. Contractor tests as required by other sections of Division 28 shall be scheduled and documented in accordance with Section 01 00 00 GENERAL REQUIREMENTS. The Commissioning Agent will witness selected Contractor tests. Contractor tests shall be completed prior to scheduling Systems Functional Performance Testing.

3.3 SYSTEMS FUNCTIONAL PERFORMANCE TESTING:

A. The Commissioning Process includes Systems Functional Performance Testing that is intended to test systems functional performance under steady state conditions, to test system reaction to changes in operating conditions, and system performance under emergency conditions. The Commissioning Agent will prepare detailed Systems Functional Performance Test procedures for review and approval by the Resident Engineer. The Contractor shall review and comment on the tests prior to approval. The Contractor shall provide the required labor, materials, and test equipment identified in the test procedure to perform the tests. The Commissioning Agent will witness and document the testing. The Contractor shall sign the test reports to verify tests were performed. See Section 01 91 00 GENERAL COMMISSIONING REQUIREMENTS, for additional details.

3.4 TRAINING OF VA PERSONNEL

A. Training of the VA’s operation and maintenance personnel is required in cooperation with the Resident Engineer and Commissioning Agent. Provide competent, factory authorized personnel to provide instruction to operation and maintenance personnel concerning the location, operation, and troubleshooting of the installed systems. The instruction shall be scheduled in coordination with the Resident Engineer after submission and approval of formal training plans. Refer to Section 01 91 00 GENERAL COMMISSIONING REQUIREMENTS and Division 28 Sections for additional Contractor training requirements.

----- END -----

SECTION 28 13 00
PHYSICAL ACCESS CONTROL SYSTEM

PART 1 – GENERAL

1.1 DESCRIPTION

A. This section specifies the finishing, installation, connection, testing and certification of a complete and fully operating Physical Access Control System, hereinafter referred to as the PACS.

B. This Section includes a Physical Access Control System consisting of a system server, one or more networked workstation computers, operating system and application software, and field-installed Controllers connected by a high-speed electronic data transmission network. The PACS shall have the following:

1. Physical Access Control:
   a. Regulating access through doors.
   b. Anti-passback
   c. Visitor assignment
   d. Surge and tamper protection
   e. Secondary alarm annunciator
   f. Credential cards and readers
   g. Biometric identity verification equipment
   h. Push-button switches
   i. RS-232 ASCII interface
   j. Credential creation and credential holder database and management
   k. Monitoring of field-installed devices
   l. Reporting
2. Security:
   a. Video and camera control.

C. System Architecture:

1. Provide server and workstation configurations with all necessary connectors, interfaces and accessories as shown.

D. PACS shall provide secure and reliable identification of Federal employees and contractors by utilizing credential authentication per FIPS-201.

E. Physical Access Control System (PACS) shall consist of:

1. Head-End equipment server,
2. One or more networked PC-based workstations,
3. Physical Access Control System and Database Management Software,

4. Credential validation software/hardware,
5. Field installed controllers,
6. PIV Middelware,
7. Card readers,
8. Biometric identification devices,
9. Supportive information system,
10. Door locks and sensors,
11. Power supplies,
12. Interfaces with:
    a. Video Surveillance and Assessment System (under alternate bid),
    b. Automatic door operators, new and existing, coordinate with VA COR.
    c. Intrusion Detection System – Coordinate with VA COR.
    d. Fire protection systems – Coordinate with VA COR.

F. Head-End equipment server, workstations and controllers shall be connected by a high-speed electronic data transmission network.

G. Information system supporting PACS, Head-End equipment server, workstations, and controllers shall comply with FIPS 200 requirements (Minimum Security Requirements for Federal Information and Information Systems)and NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems).

H. PACS system shall support:

1. Multiple credential authentication modes,
2. Bidirectional communication with the reader,
3. Incident response policy implementation capability; system shall have capability to automatically change access privileges for certain user groups to high security areas in case of incident/emergency.
4. Visitor management,

I. All security relevant decisions shall be made on “secure side of the door”. Secure side processing shall include;

1. Challenge/response management,
2. PKI path discovery and validation,
3. Credential identifier processing,
4. Authorization decisions.

J. For locations where secure side processing is not applicable the tamper switches and certified cryptographic processing shall be provided per FIPS-140-2.

K. System Software: Based on Microsoft Windows central-station, workstation operating system, server operating system, and application software.

L. Software and controllers shall be capable of matching full 56 bit FASC-N plus minimum of 32 bits of public key certificate data.

M. Software shall have the following capabilities:

1. Multiuser multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations.
2. Support authentication and enrolment;
   a. PIV verification,
   b. Expiration date check,
   c. Biometric check,
   d. Digital photo display/check,
   e. Validate digital signatures of data objects (Objects are signed by the Trusted Authority
   f. Private key challenge (CAK & PAK to verify private key public key pairs exist and card is not a clone)
3. Support CRL validation via OCSP or SCVP on a scheduled basis and automatically deny access to any revoked credential in the system.
4. Graphical user interface to show pull-down menus and a menu tree format that complies with interface guidelines of Microsoft Windows operating system.
5. System license shall be for the entire system and shall include capability for future additions that are within the indicated system size limits specified in this Section.
6. System shall have open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with Microsoft Windows operating system.
7. Operator login and access shall be utilized via integrated smart card reader and password protection.

N. Systems Networks:

1. A standalone system network shall interconnect all components of the system. This network shall include communications between a central station and any peer or subordinate workstations, enrollment

stations, local annunciation stations, portal control stations or redundant central stations.

O. Security Management System (SMS) Server Redundancy:

1. The SMS shall support multiple levels of fault tolerance and SMS redundancy listed and described below:

   a. Hot Standby Servers

   b. Clustering

   c. Disk Mirroring

   d. RAID Level 10

   e. Distributed Intelligence

P. Number of points:

1. PACS shall support multiple autonomous regional servers and/or control modules that can connect to a master command and controller server.

2. With required hardware, unlimited number of access control readers, unlimited number of inputs or outputs, unlimited number of client workstations, unlimited number of cardholders.

3. Total system solution to enable enterprise-wide, networked, multi-user access to all system resources via a wide range of options for connectivity with the customer’s existing LAN and WAN.

Q. Network(s) connecting PCs and Controllers shall comply with NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems) and consist of one or more of the following:

1. Local area, IEEE 802.3 Fast Ethernet 100 BASE-TX, star topology network based on TCP/IP.

2. Direct-connected, RS-232 cable from the COM port of the Central Station to the first Controller, then RS-485 to interconnect the remainder of the Controllers at that Location.

1.2 RELATED WORK

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.

C. Section 08 71 00 - DOOR HARDWARE. Requirements for door installation.

D. Section 26 05 11 - REQUIREMENTS FOR ELECTRICAL INSTALLATIONS. Requirements for connection of high voltage.

E. Section 26 05 21 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES (600 VOLTS AND BELOW). Requirements for power cables.

F. Section 26 05 33 – RACEWAYS AND BOXES FOR ELECTRICAL SYSTEMS. Requirements for infrastructure.

G. Section 28 05 00 - COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. For general requirements that are common to more than one section in Division 28.

H. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.

I. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.

J. Section 28 08 00 - COMMISIONING OF ELECTRONIC SAFETY AND SECURITY. For requirements for commissioning, systems readiness checklists, and training.

K. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

1.3 QUALITY ASSURANCE

A. The Contractor shall be responsible for providing, installing, and the operation of the PACS as shown. The Contractor shall also provide certification as required.

B. The security system will be installed and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, and function within existing Information Technology (IT) computer network.

C. Manufacturers Qualifications: The manufacturer shall regularly and presently produce, as one of the manufacturer's principal products, the equipment and material specified for this project, and shall have manufactured the item for at least three years.

D. Product Qualifications:

1. Manufacturer's product shall have been in satisfactory operation, on three installations of similar size and type as this project, for approximately three years.
2. The Government reserves the right to require the Contractor to submit a list of installations where the products have been in operation before approval.

E. Contractor Qualifications:

1. The Contractor or security sub-contractor shall be a licensed security Contractor with a minimum of five (5) years experience installing and servicing systems of similar scope and complexity.

The Contractor shall be an authorized regional representative of the Security Management System’s (PACS) manufacturer. The Contractor shall provide four (4) current references from clients with systems of similar scope and complexity which became operational in the past three (3) years. At least three (3) of the references shall be utilizing the same system components, in a similar configuration as the proposed system. The references must include a current point of contact, company or agency name, address, telephone number, complete system description, date of completion, and approximate cost of the project. The owner reserves the option to visit the reference sites, with the site owner’s permission and representative, to verify the quality of installation and the references’ level of satisfaction with the system. The Contractor shall provide copies of system manufacturer certification for all technicians. The Contractor shall only utilize factory-trained technicians to install, program, and service the PACS. The Contractor shall only utilize factory-trained technicians to install, terminate and service controller/field panels and reader modules. The technicians shall have a minimum of five (5) continuous years of technical experience in electronic security systems. The Contractor shall have a local service facility. The facility shall be located within 250 miles of the project site. The local facility shall include sufficient spare parts inventory to support the service requirements associated with this contract. The facility shall also include appropriate diagnostic equipment to perform diagnostic procedures. The COR reserves the option of surveying the company’s facility to verify the service inventory and presence of a local service organization.

a. The Contractor shall provide proof project superintendent with BICSI Certified Commercial Installer Level 2 to provide oversight of the project.

b. Cable installer must have on staff a Registered Communication Distribution Designer (RCDD) certified by Building Industry Consulting Service International. The staff member shall provide consistent oversight of the project cabling throughout design, layout, installation, termination and testing.

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 hours of receipt of notification that service is needed. Submit name and address of service organizations.

1.4 SUBMITTALS

A. Submit below items in conjunction with Master Specification Sections 01 33 23, SHOP DRAWINGS, PRODUCT DATA, AND SAMPLES, Section 02 41 00, DEMOLITION, and Section 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

B. Provide certificates of compliance with Section 1.3, Quality Assurance.

C. General: Submittals shall be in full compliance of the Contract Documents. All submittals shall be provided in accordance with this section. Submittals lacking the breath or depth these requirements will be considered incomplete and rejected. Submissions are considered multidisciplinary and shall require coordination with applicable divisions to provide a complete and comprehensive submission package. Additional general provisions are as follows:

1. The Contractor shall schedule submittals in order to maintain the project schedule.
2. The Contractor shall identify variations from requirements of Contract Documents and state product and system limitations, which may be detrimental to successful performance of the completed work or system.
3. Each package shall be submitted at one (1) time for each review and include components from applicable disciplines (e.g., electrical work, architectural finishes, door hardware, etc.) which are required to produce an accurate and detailed depiction of the project.
4. Manufacturer’s information used for submittal shall have pages with items for approval tagged, items on pages shall be identified, and capacities and performance parameters for review shall be clearly marked through use of an arrow or highlighting. Provide space for COR and Contractor review stamps.
5. Technical Data Drawings shall be in the latest version of AutoCAD®, drawn accurately, and in accordance with VA CAD Standards. FREEHAND SKETCHES OR COPIED VERSIONS OF THE CONSTRUCTION DOCUMENTS WILL NOT

BE ACCEPTED. The Contractor shall not reproduce Contract Documents or copy standard information as the basis of the Technical Data Drawings. If departures from the technical data drawings are subsequently deemed necessary by the Contractor, details of such departures and the reasons thereof shall be submitted in writing to the COR for approval before the initiation of work.

6. Packaging: The Contractor shall organize the submissions according to the following packaging requirements.
   a. Binders: For each manual, provide heavy duty, commercial quality, durable three (3) ring vinyl covered loose leaf binders, sized to receive 8.5 x 11 in paper, and appropriate capacity to accommodate the contents. Provide a clear plastic sleeve on the spine to hold labels describing the contents. Provide pockets in the covers to receive folded sheets.
      1) Where two (2) or more binders are necessary to accommodate data, correlate data in each binder into related groupings according to the Project Manual table of contents. Cross-referencing other binders where necessary to provide essential information for communication of proper operation and or maintenance of the component or system.
      2) Identify each binder on the front and spine with printed binder title, Project title or name, and subject matter covered. Indicate the volume number if applicable.
   b. Dividers: Provide heavy paper dividers with celluloid tabs for each Section. Mark each tab to indicate contents.
   c. Protective Plastic Jackets: Provide protective transparent plastic jackets designed to enclose diagnostic software for computerized electronic equipment.
   d. Text Material: Where written material is required as part of the manual use the manufacturer's standard printed material, or if not available, specially prepared data, neatly typewritten on 8.5 inches by 11 inches 20 pound white bond paper.
   e. Drawings: Where drawings and/or diagrams are required as part of the manual, provide reinforced punched binder tabs on the drawings and bind them with the text.
      1) Where oversized drawings are necessary, fold the drawings to the same size as the text pages and use as a foldout.

2) If drawings are too large to be used practically as a foldout, place the drawing, neatly folded, in the front or rear pocket of the binder. Insert a type written page indicating the drawing title, description of contents and drawing location at the appropriate location of the manual.
3) Drawings shall be sized to ensure details and text is of legible size. Text shall be no less than 1/16” tall.

f. Manual Content: In each manual include information specified in the individual Specification section, and the following information for each major component of building equipment and controls:
   1) General system or equipment description.
   2) Design factors and assumptions.
   3) Copies of applicable Shop Drawings and Product Data.
   4) System or equipment identification including: manufacturer, model and serial numbers of each component, operating instructions, emergency instructions, wiring diagrams, inspection and test procedures, maintenance procedures and schedules, precautions against improper use and maintenance, repair instructions, sources of required maintenance materials and related services, and a manual index.

g. Binder Organization: Organize each manual into separate sections for each piece of related equipment. At a minimum, each manual shall contain a title page, table of contents, copies of Product Data supplemented by drawings and written text, and copies of each warranty, bond, certifications, and service Contract issued. Refer to Group I through V Technical Data Package Submittal requirements for required section content.

h. Title Page: Provide a title page as the first sheet of each manual to include the following information; project name and address, subject matter covered by the manual, name and address of the Project, date of the submittal, name, address, and telephone number of the Contractor, and cross references to related systems in other operating and/or maintenance manuals.

i. Table of Contents: After the title page, include a type written table of contents for each volume, arranged systematically according to the Project Manual format. Provide a list of each product included, identified by product name or other appropriate identifying symbols and indexed to the content of the volume. Where more than one (1) volume is required to hold data for a particular system, provide a comprehensive table of contents for all volumes in each volume of the set.

j. General Information Section: Provide a general information section immediately following the table of contents, listing each product included in the manual, identified by product name. Under each product, list the name, address, and telephone number of the installer and maintenance Contractor. In addition, list a local source for replacement parts and equipment.

k. Drawings: Provide specially prepared drawings where necessary to supplement the manufacturers printed data to illustrate the relationship between components of equipment or systems, or provide control or flow diagrams. Coordinate these drawings with information contained in Project Record Drawings to assure correct illustration of the completed installation.

l. Manufacturer’s Data: Where manufacturer's standard printed data is included in the manuals, include only those sheets that are pertinent to the part or product installed. Mark each sheet to identify each part or product included in the installation. Where more than one (1) item in tabular format is included, identify each item, using appropriate references from the Contract Documents. Identify data that is applicable to the installation and delete references to information which is not applicable.

m. Where manufacturer's standard printed data is not available and the information is necessary for proper operation and maintenance of equipment or systems, or it is necessary to provide additional information to supplement the data included in the manual, prepare written text to provide the necessary information. Organize the text in a consistent format under a separate heading for different procedures. Where necessary, provide a logical sequence of instruction for each operating or maintenance procedure. Where similar or more than one product is listed on the submittal the Contractor shall differentiate by highlighting the specific product to be utilized.

n. Calculations: Provide a section for circuit and panel calculations.

o. Loading Sheets: Provide a section for DGP Loading Sheets.

p. Certifications: Provide section for Contractor's manufacturer certifications.

7. Contractor Review: Review submittals prior to transmittal. Determine and verify field measurements and field construction criteria. Verify manufacturer's catalog numbers and conformance of submittal with requirements of contract documents. Return non-conforming or incomplete submittals with requirements of the work and contract documents. Apply Contractor's stamp with signature certifying the review and verification of products occurred, and the field dimensions, adjacent construction, and coordination of information is in accordance with the requirements of the contract documents.

8. Resubmission: Revise and resubmit submittals as required within 15 calendar days of return of submittal. Make resubmissions under procedures specified for initial submittals. Identify all changes made since previous submittal.

9. Product Data: Within 15 calendar days after execution of the contract, the Contractor shall submit for approval a complete list of all of major products proposed for use. The data shall include name of manufacturer, trade name, model number, the associated contract document section number, paragraph number, and the referenced standards for each listed product.

D. Group 1 Technical Data Package: Group I Technical Data Package shall be one submittal consisting of the following content and organization. Refer to VA Special Conditions Document for drawing format and content requirements. The data package shall include the following:

1. Section I - Drawings:

a. General – Drawings shall conform to VA Special Conditions and CAD Standards Documents. All text associated with security details shall be 1/8" tall and meet VA text standard for AutoCAD™ drawings.

b. Cover Sheet – Cover sheet shall consist of Project Title and Address, Project Number, Area and Vicinity Maps.

c. General Information Sheets – General Information Sheets shall consist of General Notes, Abbreviations, Symbols, Wire and Cable Schedule, Project Phasing, and Sheet Index.

d. Floor Plans – Floor plans shall be produced from the Architectural backgrounds issued in the Construction Documents. The contractor shall receive floor plans from the prime A/E to develop these drawing sets. Security devices shall be placed on drawings in scale. All text associated with security details shall be 1/8" tall and meet VA text standard for AutoCAD™ drawings. Floor plans shall identify the following:

   1) security devices by symbol,
   2) the associated device point number (derived from the loading sheets),
   3) wire & cable types and counts
   4) conduit sizing and routing
   5) conduit riser systems
   6) device and area detail call outs

e. Architectural details – Architectural details shall be produced for each device mounting type (door details for doors with physical access control, reader pedestals and mounts, security panel and power supply details).

f. Riser Diagrams – Contractor shall provide a riser diagram indicating riser architecture and distribution of the physical access control system throughout the facility (or area in scope).

g. Block Diagrams – Contractor shall provide a block diagram for the entire system architecture and interconnections with SMS subsystems. Block diagram shall identify SMS subsystem (e.g., physical access control, intrusion detection, closed circuit television, intercom, and other associated subsystems) integration; and data transmission and media conversion methodologies.

h. Interconnection Diagrams – Contractor shall provide interconnection diagram for each sensor, and device component. Interconnection diagram shall identify termination locations, standard wire detail to include termination schedule. Diagram shall also identify interfaces to other systems such as elevator control, fire alarm systems, and security management systems.

i. Security Details:

1) Panel Assembly Detail – For each panel assembly, a panel assembly details shall be provided identifying individual panel component size and content.

2) Panel Details – Provide security panel details identify general arrangement of the security system components, backboard size, wire through size and location, and power circuit requirements.

3) Device Mounting Details – Provide mounting detailed drawing for each security device (physical access control system, intrusion detection, video surveillance and assessment, and intercom systems) for each type of wall and ceiling configuration in project. Device details shall include device, mounting detail, wiring and conduit routing.

4) Details of connections to power supplies and grounding

5) If applicable, details of surge protection device installation

6) Sensor detection patterns – Each system sensor shall have associated detection patterns.

7) Equipment Rack Detail – For each equipment rack, provide a scaled detail of the equipment rack location and rack space utilization. Use of BISCI wire management standards shall be employed to identify wire management methodology. Transitions between equipment racks shall be shown to include use vertical and horizontal latter rack system.

j. Electrical Panel Schedule – Electrical Panel Details shall be provided for all SMS systems electrical power circuits. Panel details shall be provided identifying panel type (Standard, Emergency Power, Emergency/Uninterrupted Power Source, and Uninterrupted Power Source Only), panel location, circuit number, and circuit amperage rating.

k. Door Schedule – A door schedule shall be developed for each door equipped with electronic security components. At a minimum, the door schedule shall be coordinated with Division 08 work and include the following information:

1) Item Number

2) Door Number (Derived from A/E Drawings)

3) Floor Plan Sheet Number

4) Standard Detail Number
5) Door Description (Derived from Loading Sheets)
6) Data Gathering Panel Input Number
7) Door Position or Monitoring Device Type & Model Number
8) Lock Type, Model Number & Power Input/Draw (standby/active)
9) Card Reader Type & Model Number
10) Shunting Device Type & Model Number
11) Sounder Type & Model Number
12) Manufacturer
13) Misc. devices as required
    a) Delayed Egress Type & Model Number
    b) Intercom
    c) Camera
    d) Electric Transfer Hinge
    e) Electric Pass-through device
14) Remarks column indicating special notes or door configurations

2. Section II – Data Gathering Panel Documentation Package
   a. Contractor shall provide Data Gathering Panel (DGP) input and output documentation packages for review at the Shop Drawing submittal stage and also with the as-built documentation package. The documentation packages shall be provided in both printed and magnetic form at both review stages.
   b. The Contractor shall provide loading sheet documentation package for the associated DGP, including input and output boards for all field panels associated with the project. Documentation shall be provided in current version Microsoft Excel spreadsheets following the format currently utilized by VA. A separate spreadsheet file shall be generated for each DGP and associated field panels.
   c. The spreadsheet names shall follow a sequence that shall display the spreadsheets in numerical order according to the DGP system number. The spreadsheet shall include the prefix in the file name that uniquely identifies the project site. The spreadsheet shall detail all connected items such as card readers, alarm inputs, and relay output connections. The spreadsheet shall include an individual section (row) for each panel input, output and card reader. The spreadsheet shall automatically calculate

the system numbers for card readers, inputs, and outputs based upon data entered in initialization fields.

d. All entries must be verified against the field devices. Copies of the floor plans shall be forwarded under separate cover.

e. The DGP spreadsheet shall include an entry section for the following information:

   1) DGP number
   2) First Reader Number
   3) First Monitor Point Number
   4) First Relay Number
   5) DGP, input or output Location
   6) DGP Chain Number
   7) DGP Cabinet Tamper Input Number
   8) DGP Power Fail Input Number
   9) Number of Monitor Points Reserved For Expansion Boards
   10) Number of Control Points (Relays) Reserved For Expansion Boards

f. The DGP, input module and output module spreadsheets shall automatically calculate the following information based upon the associated entries in the above fields:

   1) System Numbers for Card Readers
   2) System Numbers for Monitor Point Inputs
   3) System Numbers for Control Points (Relays)
   4) Next DGP or input module First Monitor Point Number
   5) Next DGP or output module First Control Point Number

g. The DGP spreadsheet shall provide the following information for each card reader:

   1) DGP Reader Number
   2) System Reader Number
   3) Cable ID Number
   4) Description Field (Room Number)
   5) Description Field (Device Type i.e.: In Reader, Out Reader, etc.)
   6) Description Field
   7) DGP Input Location
   8) Date Test
   9) Date Passed

10) Cable Type

11) If applicable, camera Numbers (of cameras viewing the reader location)

h. The DGP and input module spreadsheet shall provide the following information for each monitor point (alarm input).

1) DGP Monitor Point Input Number

2) System Monitor Point Number

3) Cable ID Number

4) Description Field (Room Number)

5) Description Field (Device Type i.e.: Door Contact, Motion Detector, etc.)

6) DGP or input module Input Location

7) Date Test

8) Date Passed

9) Cable Type

10) Camera Numbers (of associated alarm event preset call-ups)

i. The DGP and output module spreadsheet shall provide the following information for each control point (output relay).

1) DGP Control Point (Relay) Number

2) System (Control Point) Number

3) Cable ID Number

4) Description Field (Room Number)

5) Description Field (Device: Lock Control, Local Sounder, etc.)

6) Description Field

7) DGP or OUTPUT MODULE Output Location

8) Date Test

9) Date Passed Cable Type

10) Camera Number (of associated alarm event preset call-ups)

j. The DGP, input module and output module spreadsheet shall include the following information or directions in the header and footer:

1) Header

a) DGP Input and Output Worksheet

b) Enter Beginning Reader, Input, and Output Starting Numbers and Sheet Will Automatically Calculate the Remaining System Numbers.

2) Footer

a) File Name

b) Date Printed

c) Page Number

3. Section IV - Manufacturers' Data: The data package shall include manufacturers' data for all materials and equipment, including sensors, local processors and console equipment provided under this specification.
4. Section V - System Description and Analysis: The data package shall include system descriptions, analysis, and calculations used in sizing equipment required by these specifications. Descriptions and calculations shall show how the equipment will operate as a system to meet the performance requirements of this specification. The data package shall include the following:
   a. Central processor memory size; communication speed and protocol description; rigid disk system size and configuration; flexible disk system size and configuration; back-up media size and configuration; alarm response time calculations; command response time calculations; start-up operations; expansion capability and method of implementation; sample copy of each report specified; and color photographs representative of typical graphics.
   b. Software Data: The data package shall consist of descriptions of the operation and capability of the system, and application software as specified.
   c. Overall System Reliability Calculations: The data package shall include all manufacturers' reliability data and calculations required to show compliance with the specified reliability.
5. Section VI – Certifications & References: All specified manufacturer's certifications shall be included with the data package. Contractor shall provide Project references as outlined in Paragraph 1.4 "Quality Assurance".

E. Group II Technical Data Package

1. The Contractor shall prepare a report of "Current Site Conditions" and submit a report to the COR documenting changes to the site, particularly those conditions that affect performance of the system to be installed. The Contractor shall provide specification sheets, or written functional requirements to support the findings, and a cost estimate to correct those site changes or conditions which affect the installation of the system or its performance. The

Contractor shall not correct any deficiency without written permission from the COTR.

2. System Configuration and Functionality: The contractor shall provide the results of the meeting with VA to develop system requirements and functionality including but not limited to:
   a. Baseline configuration
   b. Access levels
   c. Schedules (intrusion detection, physical access control, holidays, etc.)
   d. Badge database
   e. System monitoring and reporting (unit level and central control)
   f. Naming conventions and descriptors

F. Group III Technical Data Package

1. Development of Test Procedures: The Contractor will prepare performance test procedures for the system testing. The test procedures shall follow the format of the VA Testing procedures and be customized to the contract requirements. The Contractor will deliver the test procedures to the COR for approval at least 60 calendar days prior to the requested test date.

G. Group IV Technical Data Package

1. Performance Verification Test
   a. Based on the successful completion of the pre-delivery test, the Contractor shall finalize the test procedures and report forms for the performance verification test (PVT) and the endurance test. The PVT shall follow the format, layout and content of the pre-delivery test. The Contractor shall deliver the PVT and endurance test procedures to the COR for approval. The Contractor may schedule the PVT after receiving written approval of the test procedures. The Contractor shall deliver the final PVT and endurance test reports within 14 calendar days from completion of the tests. Refer to Part 3 of this section for System Testing and Acceptance requirements.
2. Training Documentation
   a. New Facilities and Major Renovations: Familiarization training shall be provided for new equipment or systems. Training can include site familiarization training for VA technicians and administrative personnel. Training shall include general

information on new system layout including closet locations, turnover of the completed system including all documentation, including manuals, software, key systems, and full system administration rights. Lesson plans and training manuals training shall be oriented to type of training to be provided.

b. New Unit Control Room:

1) Provide the security personnel with training in the use, operation, and maintenance of the entire control room system (Unit Control and Equipment Rooms). The training documentation must include the operation and maintenance. The first of the training sessions shall take place prior to system turnover and the second immediately after turnover. Coordinate the training sessions with the Owner. Completed classroom sessions will be witnessed and documented by the Architect/Engineer, and approved by the COR. Instruction is not to begin until the system is operational as designed.

2) The training documents will cover the operation and the maintenance manuals and the control console operators’ manuals and service manuals in detail, stressing all important operational and service diagnostic information necessary for the maintenance and operations personnel to efficiently use and maintain all systems.

3) Provide an illustrated control console operator's manual and service manual. The operator's manual shall be written in laymen's language and printed so as to become a permanent reference document for the operators, describing all control panel switch operations, graphic symbol definitions and all indicating functions and a complete explanation of all software.

4) The service manual shall be written in laymen's language and printed so as to become a permanent reference document for maintenance personnel, describing how to run internal self diagnostic software programs, troubleshoot head end hardware and field devices with a complete scenario simulation of all possible system malfunctions and the appropriate corrective measures.

5) Provide a professional color DVD instructional recording of all the operational procedures described in the operator's manual. All charts used in the training session shall be clearly presented on the video. Any DVD found to be inferior in recording or material content shall be reproduced at no cost until an acceptable DVD is submitted. Provide four copies of the training DVD, one to the architect/engineer and three to the owner.

3. System Configuration and Data Entry:
   a. The contractor is responsible for providing all system configuration and data entry for the SMS and subsystems (e.g., video matrix switch, intercom, digital video recorders, network video recorders). All data entry shall be performed per VA standards & guidelines. The Contractor is responsible for participating in all meetings with the client to compile the information needed for data entry. These meetings shall be established at the beginning of the project and incorporated in to the project schedule as a milestone task. The contractor shall be responsible for all data collection, data entry, and system configuration. The contractor shall collect, enter, & program and/or configure the following components:
      1) Physical Access control system components,
      2) Video surveillance, control and recording systems,
      3) All other security subsystems shown in the contract documents.
   b. The Contractor is responsible for compiling the card access database for the VA employees, including programming reader configurations, access shifts, schedules, exceptions, card classes and card enrollment databases.
   c. Refer to Part 3 for system programming requirements and planning guidelines.
4. Graphics: Based on CAD as-built drawings developed for the construction project, create all map sets showing locations of all alarms and field devices. Graphical maps of all alarm points installed under this contract including perimeter and exterior alarm points shall be delivered with the system. The Contractor shall create and install all graphics needed to make the system operational. The Contractor shall utilize data from the contract

documents, Contractor’s field surveys, and all other pertinent information in the Contractor’s possession to complete the graphics. The Contractor shall identify and request from the COTR, any additional data needed to provide a complete graphics package. Graphics shall have sufficient level of detail for the system operator to assess the alarm. The Contractor shall supply hard copy, color examples at least 203.2 x 254 mm (8 x 10 in) of each type of graphic to be used for the completed Security system. The graphics examples shall be delivered to the COR for review and approval at least 90 calendar days prior to the scheduled date the Contractor requires them.

H. Group V Technical Data Package: Final copies of the manuals shall be delivered to the COR as part of the acceptance test. The draft copy used during site testing shall be updated with any changes required prior to final delivery of the manuals. Each manual’s contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of each sub-contractor installing equipment or systems, as well as the nearest service representatives for each item of equipment for each system. The manuals shall include a table of contents and tab sheets. Tab sheets shall be placed at the beginning of each chapter or section and at the beginning of each appendix. The final copies delivered after completion of the endurance test shall include all modifications made during installation, checkout, and acceptance. Six (6) hard-copies and one (1) soft copy on CD of each item listed below shall be delivered as a part of final systems acceptance.

1. Functional Design Manual: The functional design manual shall identify the operational requirements for the entire system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included for all system operating modes. Manufacturer developed literature may be used; however, shall be produced to match the project requirements.
2. Equipment Manual: A manual describing all equipment furnished including:
   a. General description and specifications; installation and checkout procedures; equipment electrical schematics and layout drawings;

system schematics and layout drawings; alignment and calibration procedures; manufacturer's repair list indicating sources of supply; and interface definition.

3. Software Manual: The software manual shall describe the functions of all software and include all other information necessary to enable proper loading, testing, and operation. The manual shall include:
   a. Definition of terms and functions; use of system and applications software; procedures for system initialization, start-up, and shutdown; alarm reports; reports generation, database format and data entry requirements; directory of all disk files; and description of all communications protocols including data formats, command characters, and a sample of each type of data transfer.
4. Operator's Manual: The operator's manual shall fully explain all procedures and instructions for the operation of the system, including:
   a. Computers and peripherals; system start-up and shutdown procedures; use of system, command, and applications software; recovery and restart procedures; graphic alarm presentation; use of report generator and generation of reports; data entry; operator commands' alarm messages, and printing formats; and system access requirements.
5. Maintenance Manual: The maintenance manual shall include descriptions of maintenance for all equipment including inspection, recommend schedules, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.
6. Spare Parts & Components Data: At the conclusion of the Contractor's work, the Contractor shall provide the COR with spare parts for each component of the completed system. Contractor shall provide the manufacturer's recommended spare parts and components required to satisfactorily maintain and service the systems, as well as unit pricing for those parts and components.
7. Operation, Maintenance & Service Manuals: The Contractor shall provide two (2) complete sets of operating and maintenance manuals in the form of an instructional manual for use by the VA Security Guard Force personnel. The manuals shall be organized into suitable

sets of manageable size. Where possible, assemble instructions for similar equipment into a single binder. If multiple volumes are required, each volume shall be fully indexed and coordinated.

8. Equipment and Systems Maintenance Manual: The Contractor shall provide the following descriptive information for each piece of equipment, operating system, and electronic system:
   a. Equipment and/or system function.
   b. Operating characteristics.
   c. Limiting conditions.
   d. Performance curves.
   e. Engineering data and test.
   f. Complete nomenclature and number of replacement parts.
   g. Provide operating and maintenance instructions including assembly drawings and diagrams required for maintenance and a list of items recommended to stock as spare parts.
   h. Provide information detailing essential maintenance procedures including the following: routine operations, trouble shooting guide, disassembly, repair and re-assembly, alignment, adjusting, and checking.
   i. Provide information on equipment and system operating procedures, including the following; start-up procedures, routine and normal operating instructions, regulation and control procedures, instructions on stopping, shut-down and emergency instructions, required sequences for electric and electronic systems, and special operating instructions.
   j. Manufacturer equipment and systems maintenance manuals are permissible.
9. Project Redlines: During construction, the Contractor shall maintain an up-to-date set of construction redlines detailing current location and configuration of the project components. The redline documents shall be marked with the words ‘Master Redlines’ on the cover sheet and be maintained by the Contractor in the project office. The Contractor will provide access to redline documents anytime during the project for review and inspection by the COR or authorized Office of Protection Services representative. Master redlines shall be neatly maintained throughout the project and secured under lock and key in the contractor’s onsite project

office. Any project component or assembly that is not installed in strict accordance with the drawings shall be so noted on the drawings. Prior to producing Record Construction Documents, the contractor will submit the Master Redline document to the COR for review and approval of all changes or modifications to the documents. Each sheet shall have COR initials indicating authorization to produce "As Built" documents. Field drawings shall be used for data gathering & field changes. These changes shall be made to the master redline documents daily. Field drawings shall not be considered "master redlines".

10. Record Specifications: The Contractor shall maintain one (1) copy of the Project Specifications, including addenda and modifications issued, for Project Record Documents. The Contractor shall mark the Specifications to indicate the actual installation where the installation varies substantially from that indicated in the Contract Specifications and modifications issued. (Note related Project Record Drawing information where applicable). The Contractor shall pay particular attention to substitutions, selection of product options, and information on concealed installations that would be difficult to identify or measure and record later. Upon completion of the mark ups, the Contractor shall submit record Specifications to the COTR. As with master relines, Contractor shall maintain record specifications for COR review and inspection at anytime.
11. Record Product Data: The Contractor shall maintain one (1) copy of each Product Data submittal for Project Record Document purposes. The Data shall be marked to indicate the actual product installed where the installation varies substantially from that indicated in the Product Data submitted. Significant changes in the product delivered to the site and changes in manufacturer's instructions and recommendations for installation shall be included. Particular attention will be given to information on concealed products and installations that cannot be readily identified or recorded later. Note related Change Orders and mark up of Record Construction Documents, where applicable. Upon completion of mark up, submit a complete set of Record Product Data to the COTR.

12. Miscellaneous Records: The Contractor shall maintain one (1) copy of miscellaneous records for Project Record Document purposes. Refer to other Specifications for miscellaneous record-keeping requirements and submittals concerning various construction activities. Before substantial completion, complete miscellaneous records and place in good order, properly identified and bound or filed, ready for use and reference. Categories of requirements resulting in miscellaneous records include, a minimum of the following:
    a. Certificates received instead of labels on bulk products.
    b. Testing and qualification of tradesmen. ("Contractor's Qualifications")
    c. Documented qualification of installation firms.
    d. Load and performance testing.
    e. Inspections and certifications.
    f. Final inspection and correction procedures.
    g. Project schedule
13. Record Construction Documents (Record As-Built)
    a. Upon project completion, the contractor shall submit the project master redlines to the COR prior to development of Record construction documents. The COR shall be given a minimum of a thirty (30) day review period to determine the adequacy of the master redlines. If the master redlines are found suitable by the COR, the COR will initial and date each sheet and turn redlines over to the contractor for as built development.
    b. The Contractor shall provide the COR a complete set of "as-built" drawings and original master redlined marked "as-built" blue-line in the latest version of AutoCAD drawings unlocked on CD or DVD. The as-built drawing shall include security device number, security closet connection location, data gathering panel number, and input or output number as applicable. All corrective notations made by the Contractor shall be legible when submitted to the COTR. If, in the opinion of the COTR, any redlined notation is not legible, it shall be returned to the Contractor for re-submission at no extra cost to the Owner. The Contractor shall organize the Record Drawing sheets into manageable sets bound with durable paper cover sheets with suitable titles,

dates, and other identifications printed on the cover. The submitted as built shall be in editable formats and the ownership of the drawings shall be fully relinquished to the owner.

c. Where feasible, the individual or entity that obtained record data, whether the individual or entity is the installer, sub-contractor, or similar entity, is required to prepare the mark up on Record Drawings. Accurately record the information in a comprehensive drawing technique. Record the data when possible after it has been obtained. For concealed installations, record and check the mark up before concealment. At the time of substantial completion, submit the Record Construction Documents to the COTR. The Contractor shall organize into bound and labeled sets for the COTR's continued usage. Provide device, conduit, and cable lengths on the conduit drawings. Exact in-field conduit placement/routings shall be shown. All conduits shall be illustrated in their entire length from termination in security closets; no arrowed conduit runs shall be shown. Pull box and junction box sizes are to be shown if larger than 100mm (4 inch).

I. FIPS 201 Compliance Certificates

1. Provide Certificates for all software components and device types utilizing credential verification. Provide certificates for:

a. Fingerprint Capture Station

b. Card Readers

d. PIV Middelware

e. Template Matcher

f. Electromagnetically Opaque Sleeve

g. Certificate Management

1) CAK Authentication System

2) PIV Authentication System

3) Certificate Validator

4) Cryptographic Module

J. Approvals will be based on complete submission of manuals together with shop drawings.

K. Completed System Readiness Checklists provided by the Commissioning Agent and completed by the contractor, signed by a qualified technician and dated on the date of completion, in accordance with the requirements of Section 28 08 00 COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

1.5 APPLICABLE PUBLICATIONS

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.........ADA Standards for Accessible Design 2010

E. Department of Veterans Affairs (VA):

PACS-R: Physical Access Control System (PACS) Requirements

VA Handbook 0730 Security and Law Enforcement

F. Government Accountability Office (GAO):

GAO-03-8-02 Security Responsibilities for Federally Owned and Leased Facilities

G. National Electrical Manufactures Association (NEMA):

250-08..................Enclosures for Electrical Equipment (1000 Volts Maximum)

H. National Fire Protection Association (NFPA):

70-11.................. National Electrical Code

I. Underwriters Laboratories, Inc. (UL):

294-99..................The Standard of Safety for Access Control System Units

305-08..................Standard for Panic Hardware

2058-05.................High Security Electronic Locks

J. Homeland Security Presidential Directive (HSPD):

HSPD-12................Policy for a Common Identification Standard for Federal Employees and Contractors

K. Federal Communications Commission (FCC):

(47 CFR 15) Part 15 Limitations on the Use of Wireless Equipment/Systems

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 800-63......Electronic Authentication Guideline

Special Pub 800-96......PIV Card Reader Interoperability Guidelines

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 800-79-1....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 800-37......Guide for Applying the Risk Management Framework to Federal Information Systems

Special Pub 800-96......PIV Card Reader Interoperability Guidelines

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. Institute of Electrical and Electronics Engineers (IEEE):

C62.41..................IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits

O. 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

19794...................Information technology - Biometric data interchange formats

P. Uniform Federal Accessibility Standards (UFAS) 1984

Q. ADA Standards for Accessible Design 2010

R. Section 508 of the Rehabilitation Act of 1973

1.6 DEFINITIONS

A. ABA Track: Magnetic stripe that is encoded on track 2, at 75-bpi density in binary-coded decimal format; for example, 5-bit, 16-character set.

B. Access Control List: A list of (identifier, permissions) pairs associated with a resource or an asset. As an expression of security policy, a person may perform an operation on a resource or asset if and only if the person's identifier is present in the access control list (explicitly or implicitly), and the permissions in the (identifier, permissions) pair include the permission to perform the requested operation.

C. Access Control: A function or a system that restricts access to authorized persons only.

D. API Application Programming Interface

E. Assurance Level (or E-Authentication Assurance Level): A measure of trust or confidence in an authentication mechanism defined in OMB Memorandum M-04-04 and NIST Special Publication (SP) 800-63, in terms of four levels: [M-04-04]

1. Level 1: LITTLE OR NO confidence
2. Level 2: SOME confidence
3. Level 3: HIGH confidence
4. Level 4: VERY HIGH confidence

F. Authentication: A process that establishes the origin of information, or determines an entity's identity. In this publication, authentication often means the performance of a PIV authentication mechanism.

G. Authenticator: A memory, possession, or quality of a person that can serve as proof of identity, when presented to a verifier of the appropriate kind. For example, passwords, cryptographic keys, and fingerprints are authenticators.

H. Authorization: A process that associates permission to access a resource or asset with a person and the person's identifier(s).

I. BIO or BIO-A: A FIPS 201 authentication mechanism that is implemented by using a Fingerprint data object sent from the PIV Card to the PACS. Note that the short-hand "BIO (-A)" is used throughout the document to represent both BIO and BIO-A authentication mechanisms.

J. Biometric: An authenticator produced from measurable qualities of a living person.

K. CAC EP – CAC End Point with end point PIV applet

L. CAC NG – CAC Next Generation with transitional PIV applet

M. Card Authentication Key (CAK): A PIV authentication mechanism (or the PIV Card key of the same name) that is implemented by an asymmetric or symmetric key challenge/response protocol. The CAK is an optional mechanism defined in NIST SP 800-73. [SP800-73] NIST strongly recommends that every PIV Card contain an asymmetric CAK and corresponding certificate, and that agencies use the asymmetric CAK protocol, rather than a symmetric CAK protocol, whenever the CAK authentication mechanism is used with PACS.

N. CCTV: Closed-circuit television.

O. Central Station: A PC with software designated as the main controlling PC of the PACS. Where this term is presented with initial capital letters, this definition applies.

P. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation. Where this term is presented with an initial capital letter, this definition applies.

Q. CPU: Central processing unit.

R. Credential: Data assigned to an entity and used to identify that entity.

S. File Server: A PC in a network that stores the programs and data files shared by users.

T. FIPS Federal Information Processing Standards

U. FRAC – First Responder Authentication Credential

V. HSPD Homeland Security Presidential Directive

W. I/O: Input/Output.

X. Identifier: A credential card, keypad personal identification number or code, biometric characteristic, or other unique identification entered as data into the entry-control database for the purpose of identifying an individual. Where this term is presented with an initial capital letter, this definition applies.

Y. IEC International Electrotechnical Commission

Z. ISO International Organization for Standardization

AA. KB Kilobyte

BB. kbit/s Kilobits / second

CC. LAN: Local area network.

DD. LED: Light-emitting diode.

EE. Legacy CAC – Contact only Common Access Card with v1 and v2 applets

FF. Location: A Location on the network having a PC-to-Controller communications link, with additional Controllers at the Location connected to the PC-to-Controller link with RS-485 communications loop.

Where this term is presented with an initial capital letter, this definition applies.

GG. NIST: National Institute of Standards and Technology

HH. PACS: Physical Access Control System

II. PC/SC: Personal Computer / Smart Card

JJ. PC: Personal computer. This acronym applies to the Central Station, workstations, and file servers.

KK. PCI Bus: Peripheral component interconnect; a peripheral bus providing a high-speed data path between the CPU and peripheral devices (such as monitor, disk drive, or network).

LL. PDF: (Portable Document Format.) The file format used by the Acrobat document exchange system software from Adobe.

MM. PIV: Personal Identification Verification

NN. PIV-I – PIV Interoperable credential

OO. PPS: Protocol and Parameters Selection

PP. RF: Radio frequency.

QQ. ROM: Read-only memory. ROM data are maintained through losses of power.

RR. RS-232: An TIA/EIA standard for asynchronous serial data communications between terminal devices. This standard defines a 25-pin connector and certain signal characteristics for interfacing computer equipment.

SS. RS-485: An TIA/EIA standard for multipoint communications.

TT. Scramble Pad: An alphanumeric keypad which randomly generates its 3-16 digit, high intensity LED keypad before each use.

TT. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

UU. TPDU: Transport Protocol Data Unit

VV. TWIC – Transportation Worker Identification Credential

WW. UPS: Uninterruptible power supply.

XX. Vcc: Voltage at the Common Collector

YY. WAN: Wide area network.

ZZ. WAV: The digital audio format used in Microsoft Windows.

AAA. Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card.

BBB. Windows: Operating system by Microsoft Corporation.

CCC. Workstation: A PC with software that is configured for specific limited security system functions.

1.7 COORDINATION

A. Coordinate arrangement, mounting, and support of electronic safety and security equipment:

1. To allow maximum possible headroom unless specific mounting heights that reduce headroom are indicated.
2. To provide for ease of disconnecting the equipment with minimum interference to other installations.
3. To allow right of way for piping and conduit installed at required slope.
4. So connecting raceways, cables, wireways, cable trays, and busways will be clear of obstructions and of the working and access space of other equipment.

B. Coordinate installation of required supporting devices and set sleeves in cast-in-place concrete, masonry walls, and other structural components as they are constructed.

C. Coordinate location of access panels and doors for electronic safety and security items that are behind finished surfaces or otherwise concealed.

1.8 MAINTENANCE & SERVICE

A. General Requirements

1. The Contractor shall provide all services required and equipment necessary to maintain the entire integrated electronic security system in an operational state as specified for a period of one (1) year after formal written acceptance of the system. The Contractor shall provide all necessary material required for performing scheduled adjustments or other non-scheduled work. Impacts on facility operations shall be minimized when performing scheduled adjustments or other non-scheduled work. See also General Project Requirements.

B. Description of Work

1. The adjustment and repair of the security system includes all software updates, panel firmware, and the following new items computers equipment, communications transmission equipment and data transmission media (DTM), local processors, security system sensors,

physical access control equipment, facility interface, signal transmission equipment, and video equipment.

C. Personnel

1. Service personnel shall be certified in the maintenance and repair of the selected type of equipment and qualified to accomplish all work promptly and satisfactorily. The COR shall be advised in writing of the name of the designated service representative, and of any change in personnel. The COR shall be provided copies of system manufacturer certification for the designated service representative.

D. Schedule of Work

1. The work shall be performed during regular working ours, Monday through Friday, excluding federal holidays. These inspections shall include:

a) The Contractor shall perform two (2) minor inspections at six (6) month intervals or more if required by the manufacturer, and two (2) major inspections offset equally between the minor inspections to effect quarterly inspection of alternating magnitude.

1) Minor Inspections shall include visual checks and operational tests of all console equipment, peripheral equipment, local processors, sensors, electrical and mechanical controls, and adjustments on printers.

2) Major Inspections shall include all work described for Minor Inspections and the following: clean all system equipment and local processors including interior and exterior surfaces; perform diagnostics on all equipment; operational tests of the CPU, switcher, peripheral equipment, recording devices, monitors, picture quality from each camera; check, walk test, and calibrate each sensor; run all system software diagnostics and correct all problems; and resolve any previous outstanding problems.

E. Emergency Service

1. The owner shall initiate service calls whenever the system is not functioning properly. The Contractor shall provide the Owner with an emergency service center telephone number. The emergency service center shall be staffed 24 hours a day 365 days a year. The Owner

shall have sole authority for determining catastrophic and non-catastrophic system failures within parameters stated in General Project Requirements.

a. For catastrophic system failures, the Contractor shall provide same day four (4) hour service response with a defect correction time not to exceed eight (8) hours from arrival on site. Catastrophic system failures are defined as any system failure that the Owner determines will place the facility(s) at increased risk.

b. For non-catastrophic failures, the Contractor within eight (8) hours with a defect correction time not to exceed 24 hours from notification.

F. Operation

1. Performance of scheduled adjustments and repair shall verify operation of the system as demonstrated by the applicable portions of the performance verification test.

G. Records & Logs

1. The Contractor shall maintain records and logs of each task and organize cumulative records for each component and for the complete system chronologically. A continuous log shall be submitted for all devices. The log shall contain all initial settings, calibration, repair, and programming data. Complete logs shall be maintained and available for inspection on site, demonstrating planned and systematic adjustments and repairs have been accomplished for the system.

H. Work Request

1. The Contractor shall separately record each service call request, as received. The record shall include the serial number identifying the component involved, its location, date and time the call was received, specific nature of trouble, names of service personnel assigned to the task, instructions describing the action taken, the amount and nature of the materials used, and the date and time of commencement and completion. The Contractor shall deliver a record of the work performed within five (5) working days after the work was completed.

I. System Modifications

1. The Contractor shall make any recommendations for system modification in writing to the COTR. No system modifications, including operating parameters and control settings, shall be made without prior written approval from the COTR. Any modifications made to the system shall be incorporated into the operation and maintenance manuals and other documentation affected.

J. Software

1. The Contractor shall provide all software updates when approved by the Owner from the manufacturer during the installation and 12-month warranty period and verify operation of the system. These updates shall be accomplished in a timely manner, fully coordinated with the system operators, and incorporated into the operations and maintenance manuals and software documentation. There shall be at least one (1) scheduled update near the end of the first year's warranty period, at which time the Contractor shall install and validate the latest released version of the Manufacturer's software. All software changes shall be recorded in a log maintained in the unit control room. An electronic copy of the software update shall be maintained within the log. At a minimum, the contractor shall provide a description of the modification, when the modification occurred, and name and contact information of the individual performing the modification. The log shall be maintained in a white 3 ring binder and the cover marked "SOFTWARE CHANGE LOG".

1.9 PERFORMANCE REQUIREMENTS

A. PACS shall provide support for multiple authentication modes and bidirectional communication with the reader. PACS shall provide implementation capability for enterprise security policy and incident response.

B. All processing of authentication information must occur on the "safe side" of a door

C. Physical Access Control System shall provide access to following Security Areas:

1. Controlled
2. Limited

D. PACS shall provide:

1. One authentication factor for access to Controlled security areas

2. Two authentication factors for access to Limited security areas

E. PACS shall provide Credential Validation and Path Validation per NIST 800-116.

F. The PACS System shall have an Enterprise Path Validation Module (PVM) component that processes X.509 certification paths composed of X.509 v3 certificates and X.509 v2 CRLs. The PVM component MUST support the following features:

1. Name chaining;
2. Signature chaining;
3. Certificate validity;
4. Key usage, basic constraints, and certificate policies certificate extensions;
5. Full CRLs; and
6. CRLs segmented on names.

G. Distributed Processing: System shall be a fully distributed processing system so that information, including time, date, valid codes, access levels, and similar data, is downloaded to Controllers so that each Controller makes access-control decisions for that Location. Do not use intermediate Controllers for physical access control. If communications to Central Station are lost, all Controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the Central Station.

H. Data Capacity:

1. 130 different card-reader formats.
2. 999 comments.
3. 16 graphic file types for importing maps.

I. Location Capacity:

1. 512 Base bid, 128 de-duct bid, reader-controlled doors.
2. 50,000 total access credentials.
3. 2048 supervised alarm inputs.
4. 2048 programmable outputs.
5. 32,000 custom action messages per Location to instruct operator on action required when alarm is received.

J. System Network Requirements:

1. Interconnect system components and provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.
2. Communication shall not require operator initiation or response, and shall return to normal after partial or total network interruption such as power loss or transient upset.
3. System shall automatically annunciate communication failures to the operator and identify the communication link that has experienced a partial or total failure.
4. Communications Controller may be used as an interface between the Central Station display systems and the field device network. Communications Controller shall provide functions required to attain the specified network communications performance.

K. Central Station shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring. Central Station shall control system networks to interconnect all system components, including workstations and field-installed Controllers.

L. Field equipment shall include Controllers, sensors, and controls. Controllers shall serve as an interface between the Central Station and sensors and controls. Data exchange between the Central Station and the Controllers shall include down-line transmission of commands, software, and databases to Controllers. The up-line data exchange from the Controller to the Central Station shall include status data such as intrusion alarms, status reports, and entry-control records. Controllers are classified as alarm-annunciation or entry-control type.

M. System Response to Alarms: Field device network shall provide a system end-to-end response time of 1 second or less for every device connected to the system. Alarms shall be annunciated at the Central Station within 1 second of the alarm occurring at a Controller or device controlled by a local Controller, and within 100 ms if the alarm occurs at the Central Station. Alarm and status changes shall be displayed within 100 ms after receipt of data by the Central Station. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within 5 seconds of alarm receipt at the security console.

N. False Alarm Reduction: The design of Central Station and Controllers shall contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.

O. Error Detection: A cyclic code error detection method shall be used between Controllers and the Central Station, which shall detect single- and double-bit errors, burst errors of eight bits or less, and at least 99 percent of all other multibit and burst error conditions. Interactive or product error detection codes alone will not be acceptable. A message shall be in error if one bit is received incorrectly. System shall retransmit messages with detected errors. A two-digit decimal number shall be operator assignable to each communication link representing the number of retransmission attempts. When the number of consecutive retransmission attempts equals the assigned quantity, the Central Station shall print a communication failure alarm message. System shall monitor the frequency of data transmission failure for display and logging.

P. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.

Q. Door Hardware Interface: Coordinate with Division 08 Sections that specify door hardware required to be monitored or controlled by the PACS. The Controllers in this Section shall have electrical characteristics that match the signal and power requirements of door hardware. Integrate door hardware specified in Division 08 Sections to function with the controls and PC-based software and hardware in this Section.

R. References to industry and trade association standards and codes are minimum installation requirement standards.

S. Drawings and other specification sections shall govern in those instances where requirements are greater than those specified in the above standards.

1.10 EQUIPMENT AND MATERIALS

A. Materials and equipment furnished shall be of current production by manufacturers regularly engaged in the manufacture of such items, for which replacement parts shall be available.

B. When more than one unit of the same class of equipment is required, such units shall be the product of a single manufacturer.

C. Equipment Assemblies and Components:

1. Components of an assembled unit need not be products of the same manufacturer.
2. Manufacturers of equipment assemblies, which include components made by others, shall assume complete responsibility for the final assembled unit.
3. Components shall be compatible with each other and with the total assembly for the intended service.
4. Constituent parts which are similar shall be the product of a single manufacturer.

D. Factory wiring shall be identified on the equipment being furnished and on all wiring diagrams.

E. When Factory Testing Is Specified:

1. The Government shall have the option of witnessing factory tests. The contractor shall notify the VA through the COR a minimum of 15 working days prior to the manufacturers making the factory tests.
2. Four copies of certified test reports containing all test data shall be furnished to the COR prior to final inspection and not more than 90 days after completion of the tests.
3. When equipment fails to meet factory test and re-inspection is required, the contractor shall be liable for all additional expenses, including expenses of the Government.

F. For each controller/module/device provided as part of the PACS, the contractor shall provide 10% of the total number of controller/module/device provided.

1.11 WARRANTY OF CONSTRUCTION.

A. Warrant PACS work subject to the Article “Warranty of Construction” of FAR clause 52.246-21.

B. Demonstration and training shall be performed prior to system acceptance.

1.12 GENERAL REQUIREMENTS

A. For general requirements that are common to more than one section in Division 28 refer to Section 28 05 00, REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY INSTALLATIONS.

B. General requirements applicable to this section include:

1. General Arrangement Of Contract Documents,
2. Delivery, Handling and Storage,
3. Project Conditions,

4. Electrical Power,
5. Grounding,
6. Electronic Components,
7. Substitute Materials and Equipment, and
8. Like Items.

PART 2 – PRODUCTS

2.1 GENERAL

A. All equipment and materials for the system will be compatible to ensure correct operation as outlined in FIPS 201, March 2006 and HSPD-12.

B. The security system characteristics listed in this section will serve as a guide in selection of equipment and materials for the PACS. If updated or more suitable versions are available then the Contracting Officer will approve the acceptance of prior to an installation.

C. PACS equipment shall meet or exceed all requirements listed below.

D. A PACS shall be comprised of, but not limited to, the following components:

1. Physical Access Control System
2. Application Software
3. System Database
4. Surge and Tamper Protection
5. Standard Workstation Hardware
6. Communications Workstation
7. Controllers (Data Gathering Panel)
8. Secondary Alarm Annunciator
9. Card Readers
10. Credential Cards
11. Biometric Identity Verification Equipment
12. Biometric Enrolment Center (To be provided in accordance with the VA PIV enrollment and issuance system.)
13. System Sensors and Related Equipment
14. Push Button Switches
15. Interfaces
16. Door Hardware interface
17. RS-232 ASCII Interface
18. Video and Camera Control
19. Cables
20. Transformers

2.2 MANUFACTURER'S

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:

1. Lenel – OnGuard
2. Hirsch – Velocity
3. General Electrical – Facility Commander
4. Johnson Controls – P2000
5. Software House – C*Cure 9000

2.3 SECURITY MANAGEMENT SYSTEM (SMS)

A. Shall allow the configuration of an enrollment and badging, alarm monitoring, administrative, asset management, digital video management, visitor enrollment, remote access level management, and integrated client workstations or any combination of all or some.

B. Shall be expandable to support an unlimited number of individual module or integrated client workstations. All access control field hardware, including Data Gathering Panels(DGP), shall be connected to all physical access control system workstation on the network.

C. Shall have the ability to compose, file, maintain, update, and print reports for either individuals or the system as follows.

1. Individual reports that consist of an employee’s name, office location, phone number or direct extension, and normal hours of operation. The report shall provide a detail listing of the employee’s daily events in relation to accessing points within a facility.
2. System reports shall be able to produce information on a daily/weekly/monthly basis for all events, alarms, and any other activity associated with a system user.

D. All reports shall be in a date/time format and all information shall be clearly presented. Shall be designed to allow it to work with any industry standard network protocol and topology listed below:

1. Transmission Control Protocol (TCP)/IP
2. Novell Netware (IPX/SPX)
3. Banyan VINES
4. IBM LAN Server (NetBEUI)
5. Microsoft LAN Manager (NetBEUI)
6. Network File System (NFS) Networks

7. Remote Access Service (RAS) via ISDN, x.25, and standard phone lines.

E. Shall provide full interface and control of the PACS to include the following subsystems within the PACS:

1. Public Key Infrastructure
2. Card Management
3. Identity and Access Management
4. Personal Identity Verification

F. Shall have the following features or compatibilities:

1. The ability to be operated locally or remotely via a LAN, WAN, internet, or intranet.
2. Event and Alarm Monitoring
3. Database Partitioning
4. Ability to fully integrate with all other security subsystems
5. Enhanced Monitoring Station with Split Screen Views
6. Alternate and Extended Shunt by Door
7. Escort Management
8. Enhanced IT-based Password Protection
10. N-man Rule and Occupancy Restrictions
11. Open Journal Data Format for Enhanced Reporting
12. Automated Personnel Import
13. ODBC Support
14. Windows 2008 Server R2 or Windows 7 (Confirm software with Hospital IT staff).
15. Field-Level Audit Trail
16. Cardholder Access Events

G. System Software: Based on 32-bit, Microsoft Windows central-station and workstation operating system and application software. Confirm exact requirements with hospital IT staff before providing software. Software shall have the following features:

1. Multiuser multitasking to allow independent activities and monitoring to occur simultaneously at different workstations.
2. Graphical user interface to show pull-down menus and a menu tree format.
3. Capability for future additions within the indicated system size limits.

4. Open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with operating system.
5. Password-protected operator and smart card login and access.

H. Peer Computer Control Software: Shall detect a failure of a central computer, and shall cause the other central computer to assume control of all system functions without interruption of operation. Drivers shall be provided in both central computers to support this mode of operation.

I. Application Software: Interface between the alarm annunciation and entry-control Controllers, to monitor sensors, operate displays, report alarms, generate reports, and help train system operators. Software shall have the following functions:

1. Resides at the Central Station, workstations, and Controllers as required to perform specified functions.
2. Operate and manage peripheral devices.
3. Manage files for disk I/O, including creating, deleting, and copying files; and automatically maintain a directory of all files, including size and location of each sequential and random-ordered record.
4. Import custom icons into graphics views to represent alarms and I/O devices.
5. Globally link I/O so that any I/O can link to any other I/O within the same Location, without requiring interaction with the host PC. This operation shall be at the Controller.
6. Globally code I/O links so that any access-granted event can link to any I/O with the same Location without requiring interaction with the host PC. This operation shall be at the Controller.
7. Messages from PC to Controllers and Controllers to Controllers shall be on a polled network that utilizes check summing and acknowledgment of each message. Communication shall be automatically verified, buffered, and retransmitted if message is not acknowledged.
8. Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-Controller communications methods by changing the polling frequency and the amount of time the system waits for a response.

9. Automatic and encrypted backups for database and history backups shall be automatically stored at a selected workstation and encrypted with a nine-character alphanumeric password, which must be used to restore or read data contained in backup.
10. Operator audit trail for recording and reporting all changes made to database and system software.

J. Workstation Software:

1. Password levels shall be individually customized at each workstation to allow or disallow operator access to program functions for each Location.
2. Workstation event filtering shall allow user to define events and alarms that will be displayed at each workstation. If an alarm is unacknowledged (not handled by another workstation) for a preset amount of time, the alarm will automatically appear on the filtered workstation.

K. Report Generator Software: Include commands to generate reports for displaying, printing, and storing on disk and tape. Reports shall be stored by type, date, and time. Report printing shall be the lowest priority activity. Report generation mode shall be operator selectable but set up initially as periodic, automatic, or on request. Include time and date printed and the name of operator generating the report. Report formats may be configured by operators.

1. Automatic Printing: Setup shall specify, modify, or inhibit the report to be generated; the time the initial report is to be generated; the time interval between reports; the end of period; and the default printer.
2. Printing on Requests: An operator may request a printout of any report.
3. Alarm Reports: Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm such as door alarm, intrusion alarm, tamper alarm, etc.), the type of sensor, the location, the time, and the action taken.
4. Access and Secure Reports: Document zones placed in access, the time placed in access, and the time placed in secure mode.

5. Custom Reports: Reports tailored to exact requirements of who, what, when, and where. As an option, custom report formats may be stored for future printing.
6. Automatic History Reports: Named, saved, and scheduled for automatic generation.
7. Cardholder Reports: Include data, or selected parts of the data, as well as the ability to be sorted by name, card number, imprinted number, or by any of the user-defined fields.
8. Cardholder by Reader Reports: Based on who has access to a specific reader or group of readers by selecting the readers from a list.
9. Cardholder by Access-Level Reports: Display everyone that has been assigned to the specified access level.
10. Who Is In (Muster) Report:
    a. Emergency Muster Report: One click operation on toolbar launches report.
    b. Cardholder Report. Contain a count of persons that are "In" at a selected Location and a count with detailed listing of name, date, and time of last use, sorted by the last reader used or by the group assignment.
11. Panel Labels Reports: Printout of control-panel field documentation including the actual location of equipment, programming parameters, and wiring identification. Maintain system installation data within system database so that they are available on-site at all times.
12. Activity and Alarm On-Line Printing: Activity printers for use at workstations; prints all events or alarms only.
13. History Reports: Custom reports that allows the operator to select any date, time, event type, device, output, input, operator, Location, name, or cardholder to be included or excluded from the report.
    a. Initially store history on the hard disk of the host PC.
    b. Permit viewing of the history on workstations or print history to any system printer.
    c. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.

d. Each report shall depict the date, time, event type, event description, device, or I/O name, cardholder group assignment, and cardholder name or code number.

e. Each line of a printed report shall be numbered to ensure that the integrity of the report has not been compromised.

f. Total number of lines of the report shall be given at the end of the report. If the report is run for a single event such as "Alarms," the total shall reflect how many alarms occurred during that period.

14. Reports shall have the following four options:

a. View on screen.

b. Print to system printer. Include automatic print spooling and "Print To" options if more than one printer is connected to system.

c. "Save to File" with full path statement.

d. System shall have the ability to produce a report indicating status of system inputs and outputs or of inputs and outputs that are abnormal, out of time zone, manually overridden, not reporting, or in alarm.

15. Custom Code List Subroutine: Allow the access codes of system to be sorted and printed according to the following criteria:

a. Active, inactive, or future activate or deactivate.

b. Code number, name, or imprinted card number.

c. Group, Location, access levels.

d. Start and stop code range.

e. Codes that have not been used since a selectable number of days.

f. In, out, or either status.

g. Codes with trace designation.

16. The reports of system database shall allow options so that every data field may be printed.

17. The reports of system database shall be constructed so that the actual position of the printed data shall closely match the position of the data on the data-entry windows.

L. Training Software: Enables operators to practice system operation including alarm acknowledgment, alarm assessment, response force deployment, and response force communications. System shall continue normal operation during training exercises and shall terminate exercises when an alarm signal is received at the console.

M. Entry-Control Enrollment Software: Database management functions that allow operators to add, delete, and modify access data as needed.

1. The enrollment station shall not have alarm response or acknowledgment functions.
2. Provide multiple, password-protected access levels. Database management and modification functions shall require a higher operator access level than personnel enrollment functions.
3. The program shall provide means to disable the enrollment station when it is unattended to prevent unauthorized use.
4. The program shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations. In the case of personnel identity verification subsystems, this shall include biometric data. Allow entry of personnel identifying information into the system database using menu selections and data fields. The data field names shall be customized during setup to suit user and site needs. Personnel identity verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files.
5. Cardholder Data: Provide 99 user-defined fields. System shall have the ability to run searches and reports using any combination of these fields. Each user-defined field shall be configurable, using any combination of the following features:
   a. MASK: Determines a specific format that data must comply with.
   b. REQUIRED: Operator is required to enter data into field before saving.
   c. UNIQUE: Data entered must be unique.
   d. DEACTIVATE DATE: Data entered will be evaluated as an additional deactivate date for all cards assigned to this cardholder.
   e. NAME ID: Data entered will be considered a unique ID for the cardholder.
6. Personnel Search Engine: A report generator with capabilities such as search by last name, first name, group, or any predetermined user-defined data field; by codes not used in definable number of days; by skills; or by seven other methods.

7. Multiple Deactivate Dates for Cards: User-defined fields to be configured as additional stop dates to deactivate any cards assigned to the cardholder.
8. Batch card printing.
9. Default card data can be programmed to speed data entry for sites where most card data are similar.
10. Enhanced ACSII File Import Utility: Allows the importing of cardholder data and images.
11. Card Expire Function: Allows readers to be configured to deactivate cards when a card is used at selected devices.

N. System test software enables operators to initiate a test of the entire system or of a particular portion of the system.

1. Test Report: The results of each test shall be stored for future display or printout. The report shall document the operational status of system components.

O. Controller Software:

1. Controllers shall operate as an autonomous intelligent processing unit. Controllers shall make decisions about physical access control, alarm monitoring, linking functions, and door locking schedules for its operation, independent of other system components. Controllers shall be part of a fully distributed processing control network. The portion of the database associated with a Controller and consisting of parameters, constraints, and the latest value or status of points connected to that Controller, shall be maintained in the Controller.
2. Functions: The following functions shall be fully implemented and operational within each Controller:
   a. Monitoring inputs.
   b. Controlling outputs.
   c. Automatically reporting alarms to the Central Station.
   d. Reporting of sensor and output status to Central Station on request.
   e. Maintaining real time, automatically updated by the Central Station at least once a day.
   f. Communicating with the Central Station.
   g. Executing Controller resident programs.
   h. Diagnosing.

i. Downloading and uploading data to and from the Central Station.

3. Controller Operations at a Location:

a. Location: Ability to have a minimum of 32 Controllers connected to RS-485 communications loop. Globally operating I/O linking and anti-passback functions between Controllers within the same Location without central-station or workstation intervention. All operations, including Linking and anti-passback, shall remain fully functional within the same Location even when the Central Station or workstations are off line.

b. In the event of communications failure between the Central Station and a Location, there shall be no degradation in operations at the Controllers at that Location. The Controllers at each Location shall be connected to a memory buffer with a capacity to store up to 10,000 events; there shall be no loss of transactions in system history files until the buffer overflows.

c. Buffered events shall be handled in a first-in-first-out mode of operation.

4. Individual Controller Operation:

a. Controllers shall transmit alarms, status changes, and other data to the Central Station when communications circuits are operable. If communications are not available, Controllers shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the Central Station, shall be stored for later transmission to the Central Station. Storage capacity for the latest 1024 events shall be provided at each Controller.

b. Card-reader ports of a Controller shall be custom configurable for at least 120 different card-reader or keypad formats. Multiple reader or keypad formats may be used simultaneously at different Controllers or within the same Controller.

c. Controllers shall provide a response to card-readers or keypad entries in less than 0.25 seconds, regardless of system size.

d. Controllers that are reset, or powered up from a nonpowered state, shall automatically request a parameter download and reboot to its proper working state. This shall happen without any operator intervention.

e. Initial Startup: When Controllers are brought on-line, database parameters shall be automatically downloaded to them. After initial download is completed, only database changes shall be downloaded to each Controller.

f. Failure Mode: On failure for any reason, Controllers shall perform an orderly shutdown and force Controller outputs to a predetermined failure mode state, consistent with the failure modes shown and the associated control device.

g. Startup After Power Failure: After power is restored, startup software shall initiate self-test diagnostic routines, after which Controllers shall resume normal operation.

h. Startup After Controller Failure: On failure, if the database and application software are no longer resident, Controllers shall not restart, but shall remain in the failure mode until repaired. If database and application programs are resident, Controllers shall immediately resume operation. If not, software shall be restored automatically from the Central Station.

5. Communications Monitoring:

a. System shall monitor and report status of RS-485 communications loop of each Location.

b. Communication status window shall display which Controllers are currently communicating, a total count of missed polls since midnight, and which Controller last missed a poll.

c. Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM memory for each Controller.

6. Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month. The real-time clock shall be automatically synchronized with the Central Station at least once a day to plus or minus 10 seconds. The time synchronization shall be automatic, without operator action and without requiring system shutdown.

P. PC-to-Controller Communications:

1. Central-station or workstation communications shall use the following:

a. Direct connection using serial ports of the PC.

b. TCP/IP LAN network interface cards.

2. Serial Port Configuration: Each serial port used for communications shall be individually configurable for "direct communications," "modem communications incoming and outgoing," or "modem communications incoming only"; or as an ASCII output port.
3. Multiport Communications Board: Use if more than two serial ports are needed.
   a. Expandable and modular design. Use a 4-, 8-, or 16-serial port configuration that is expandable to 32 or 64 serial ports.
   b. Connect the first board to an internal PCI bus adapter card.
4. Direct serial and TCP/IP communications shall be alike in the monitoring or control of system.
5. TCP/IP network interface card shall have an option to set the poll frequency and message response time-out settings.
6. PC-to-Controller and Controller-to-Controller communications (direct or TCP/IP) shall use a polled-communication protocol that checks sum and acknowledges each message. All communications shall be verified and buffered and retransmitted if not acknowledged.
7. Direct Serial or TCP/IP PC-to-Controller Communications:
   a. Communication software on the PC shall supervise the PC-to-Controller communications link.
   b. Loss of communications to any Controller shall result in an alarm at all PCs running the communications software.
   c. When communications are restored, all buffered events shall automatically upload to the PC, and any database changes shall be automatically sent to the Controller.

Q. Controller-to-Controller Communications:
1. Controller-to-Controller Communications: RS-485, 4-wire, point-to-point, regenerative (repeater) communications network methodology.
2. RS-485 communications signal shall be regenerated at each Controller.

R. Database Downloads:
1. All data transmissions from PCs to a Location, and between Controllers at a Location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.

2. If a Controller is reset for any reason, it shall automatically request and receive a database download from the PC. The download shall restore data stored at the Controller to their normal working state and shall take place with no operator intervention.

S. Operator Interface:

1. Inputs in system shall have two icon representations, one for the normal state and one for the abnormal state.
2. When viewing and controlling inputs, displayed icons shall automatically change to the proper icon to display the current system state in real time. Icons shall also display the input's state, whether armed or bypassed, and if the input is in the armed or bypassed state due to a time zone or a manual command.
3. Outputs in system shall have two icon representations, one for the secure (locked) state and one for the open (unlocked) state.
4. Icons displaying status of the I/O points shall be constantly updated to show their current real-time condition without prompting by the operator.
5. The operator shall be able to scroll the list of I/Os and press the appropriate toolbar button, or right click, to command the system to perform the desired function.
6. Graphic maps or drawings containing inputs, outputs, and override groups shall include the following:
   a. Database to import and store full-color maps or drawings and allow for input, output, and override group icons to be placed on maps.
   b. Maps to provide real-time display animation and allow for control of points assigned to them.
   c. System to allow inputs, outputs, and override groups to be placed on different maps.
   d. Software to allow changing the order or priority in which maps will be displayed.
7. Override Groups Containing I/Os:
   a. System shall incorporate override groups that provide the operator with the status and control over user-defined "sets" of I/Os with a single icon.
   b. Icon shall change automatically to show the live summary status of points in that group.

c. Override group icon shall provide a method to manually control or set to time zone points in the group.

d. Override group icon shall allow the expanding of the group to show icons representing the live status for each point in the group, individual control over each point, and the ability to compress the individual icons back into one summary icon.

8. Schedule Overrides of I/Os and Override Groups:

a. To accommodate temporary schedule changes that do not fall within the holiday parameters, the operator shall have the ability to override schedules individually for each input, output, or override group.

b. Each schedule shall be composed of a minimum of two dates with separate times for each date.

c. The first time and date shall be assigned the override state that the point shall advance to, when the time and date become current.

d. The second time and date shall be assigned the state that the point shall return to, when the time and date become current.

9. Copy command in database shall allow for like data to be copied and then edited for specific requirements, to reduce redundant data entry.

T. Operator Access Control:

1. Control operator access to system controls through three password-protected operator levels. System operators and managers with appropriate password clearances shall be able to change operator levels for operators.

2. Three successive attempts by an operator to execute functions beyond their defined level during a 24-hour period shall initiate a software tamper alarm.

3. A minimum of 32 passwords shall be available with the system software. System shall display the operator's name or initials in the console's first field. System shall print the operator's name or initials, action, date, and time on the system printer at login and logoff.

4. The password shall not be displayed or printed.

5. Each password shall be definable and assignable for the following:

a. Commands usable.

b. Access to system software.

c. Access to application software.

d. Individual zones that are to be accessed.

e. Access to database.

U. Operator Commands:

1. Command Input: Plain-language words and acronyms shall allow operators to use the system without extensive training or data-processing backgrounds. System prompts shall be a word, a phrase, or an acronym.

2. Command inputs shall be acknowledged and processing shall start in not less than 1 second(s).

3. Tasks that are executed by operator's commands shall include the following:

a. Acknowledge Alarms: Used to acknowledge that the operator has observed the alarm message.

b. Place Zone in Access: Used to remotely disable intrusion alarm circuits emanating from a specific zone. System shall be structured so that console operator cannot disable tamper circuits.

c. Place Zone in Secure: Used to remotely activate intrusion alarm circuits emanating from a specific zone.

d. System Test: Allows the operator to initiate a system-wide operational test.

e. Zone Test: Allows the operator to initiate an operational test for a specific zone.

f. Print reports.

g. Change Operator: Used for changing operators.

h. Display Graphics: Used to display any graphic displays implemented in the system. Graphic displays shall be completed within 20 seconds from time of operator command.

i. Run system tests.

j. Generate and format reports.

k. Request help with the system operation.

1) Include in main menus.

2) Provide unique, descriptive, context-sensitive help for selections and functions with the press of one function key.

3) Provide navigation to specific topic from within the first help window.

4) Help shall be accessible outside the applications program.

l. Entry-Control Commands:

1) Lock (secure) or unlock (open) each controlled entry and exit up to a quantity of times as directed by hospital through time-zone programming.

2) Arm or disarm each monitored input up to a quantity of times as directed by hospital through time-zone programming.

3) Enable or disable readers or keypads up to a quantity of times as directed by hospital through time-zone programming.

4) Enable or disable cards or codes up to a quantity of times as directed by hospital per entry point through access-level programming.

4. Command Input Errors: Show operator input assistance when a command cannot be executed because of operator input errors. Assistance screen shall use plain-language words and phrases to explain why the command cannot be executed. Error responses that require an operator to look up a code in a manual or other document are not acceptable. Conditions causing operator assistance messages include the following:

a. Command entered is incorrect or incomplete.

b. Operator is restricted from using that command.

c. Command addresses a point that is disabled or out of service.

d. Command addresses a point that does not exist.

e. Command is outside the system's capacity.

V. Alarms:

1. System Setup:

a. Assign manual and automatic responses to incoming point status change or alarms.

b. Automatically respond to input with a link to other inputs, outputs, operator-response plans, unique sound with use of WAV files, and maps or images that graphically represent the point location.

c. 60-character message field for each alarm.

d. Operator-response-action messages shall allow message length of at least 65,000 characters, with database storage capacity of up to 32,000 messages. Setup shall assign messages to access point, zone, and sensors.

e. Secondary messages shall be assignable by the operator for printing to provide further information and shall be editable by the operator.

f. Allow 25 secondary messages with a field of 4 lines of 60 characters each.

g. Store the most recent 1000 alarms for recall by the operator using the report generator.

2. Software Tamper:

a. Annunciate a tamper alarm when unauthorized changes to system database files are attempted. Three consecutive unsuccessful attempts to log onto system shall generate a software tamper alarm.

b. Annunciate a software tamper alarm when an operator or other individual makes three consecutive unsuccessful attempts to invoke functions beyond their authorization level.

c. Maintain a transcript file of the last 5000 commands entered at the each Central Station to serve as an audit trail. System shall not allow write access to system transcript files by any person, regardless of their authorization level.

d. Allow only acknowledgment of software tamper alarms.

3. Read access to system transcript files shall be reserved for operators with the highest password authorization level available in system.

4. Animated Response Graphics: Highlight alarms with flashing icons on graphic maps; display and constantly update the current status of alarm inputs and outputs in real time through animated icons.

5. Multimedia Alarm Annunciation: WAV files to be associated with alarm events for audio annunciation or instructions.

6. Alarm Handling: Each input may be configured so that an alarm cannot be cleared unless it has returned to normal, with options of requiring the operator to enter a comment about disposition of alarm. Allow operator to silence alarm sound when alarm is acknowledged.

7. CCTV Alarm Interface: If applicable, allow commands to be sent to CCTV systems during alarms (or input change of state) through serial ports.
9. Camera Control: Provides operator ability to select and control cameras from graphic maps.

W. Alarm Monitoring: Monitor sensors, Controllers, and notify operators of an alarm condition. Display higher-priority alarms first and, within alarm priorities, display the oldest unacknowledged alarm first. Operator acknowledgment of one alarm shall not be considered acknowledgment of other alarms nor shall it inhibit reporting of subsequent alarms.

1. Displayed alarm data shall include type of alarm, location of alarm, and secondary alarm messages.
2. Printed alarm data shall include type of alarm, location of alarm, date and time (to nearest second) of occurrence, and operator responses.
3. Maps shall automatically display the alarm condition for each input assigned to that map, if that option is selected for that input location.
4. Alarms shall be able to be sent to, user configurable, email addresses as well as text messages.
5. Alarms initiate a status of "pending" and require the following two handling steps by operators:
    a. First Operator Step: "Acknowledged." This action shall silence sounds associated with the alarm. The alarm remains in the system "Acknowledged" but "Un-Resolved."
    b. Second Operator Step: Operators enter the resolution or operator comment, giving the disposition of the alarm event. The alarm shall then clear.
6. Each workstation shall display the total pending alarms and total unresolved alarms.
7. Each alarm point shall be programmable to disallow the resolution of alarms until the alarm point has returned to its normal state.
8. Alarms shall transmit to Central Station in real time, except for allowing connection time for dial-up locations.
9. Alarms shall be displayed and managed from a minimum of four different windows.

a. Input Status Window: Overlay status icon with a large red blinking icon. Selecting the icon will acknowledge the alarm.

b. History Log Transaction Window: Display name, time, and date in red text. Selecting red text will acknowledge the alarm.

c. Alarm Log Transaction Window: Display name, time, and date in red. Selecting red text will acknowledge the alarm.

d. Graphic Map Display: Display a steady colored icon representing each alarm input location. Change icon to flashing red when the alarm occurs. Change icon from flashing red to steady red when the alarm is acknowledged.

9. Once an alarm is acknowledged, the operator shall be prompted to enter comments about the nature of the alarm and actions taken. Operator's comments may be manually entered or selected from a programmed predefined list, or a combination of both.

10. For locations where there are regular alarm occurrences, provide programmed comments. Selecting that comment shall clear the alarm.

11. The time and name of the operator who acknowledged and resolved the alarm shall be recorded in the database.

12. Identical alarms from same alarm point shall be acknowledged at same time the operator acknowledges the first alarm. Identical alarms shall be resolved when the first alarm is resolved.

13. Alarm functions shall have priority over downloading, retrieving, and updating database from workstations and Controllers.

14. When a reader-controlled output (relay) is opened, the corresponding alarm point shall be automatically bypassed.

X. Monitor Display: Display text and graphic maps that include zone status integrated into the display. Colors are used for the various components and current data. Colors shall be uniform throughout the system.

1. Color Code:

a. FLASHING RED: Alerts operator that a zone has gone into an alarm or that primary power has failed.

b. STEADY RED: Alerts operator that a zone is in alarm and alarm has been acknowledged.

c. YELLOW: Advises operator that a zone is in access.

d. GREEN: Indicates that a zone is secure and that power is on.

2. Graphics:
   a. Support 32,000 graphic display maps and allow import of maps from a minimum of 16 standard formats from another drawing or graphics program.
   b. Allow I/O to be placed on graphic maps by the drag-and-drop method.
   c. Operators shall be able to view the inputs, outputs, and the point's name by moving the mouse cursor over the point on graphic map.
   d. Inputs or outputs may be placed on multiple graphic maps. The operator shall be able to toggle to view graphic map associated with inputs or outputs.
   e. Each graphic map shall have a display-order sequence number associated with it to provide a predetermined order when toggled to different views.
   f. Camera icons shall have the ability to be placed on graphic maps that, when selected by an operator, will open a video window, display the camera associated with that icon, and provide pan-tilt-zoom control.
   g. Input, output, or camera placed on a map shall allow the ability to arm or bypass an input, open or secure an output, or control the pan-tilt-zoom function of the selected camera.

Y. Anti-Passback:
1. System shall have global and local anti-passback features, selectable by Location. System shall support hard and soft anti-passback.
2. Hard Anti-Passback: Once a credential holder is granted access through a reader with one type of designation (IN or OUT), the credential holder may not pass through that type of reader designation until the credential holder passes though a reader of opposite designation.
3. Soft Anti-Passback: Should a violation of the proper IN or OUT sequence occur, access shall be granted, but a unique alarm shall be transmitted to the control station, reporting the credential holder and the door involved in the violation. A separate report may be run on this event.

4. Timed Anti-Passback: A Controller capability that prevents an access code from being used twice at the same device (door) within a user-defined amount of time.
5. Provide four separate zones per Location that can operate without requiring interaction with the host PC (done at Controller). Each reader shall be assignable to one or all four anti-passback zones. In addition, each anti-passback reader can be further designated as "Hard," "Soft," or "Timed" in each of the four anti-passback zones. The four anti-passback zones shall operate independently.
6. The anti-passback schemes shall be definable for each individual door.
7. The Master Access Level shall override anti-passback.
8. System shall have the ability to forgive (or reset) an individual credential holder or the entire credential holder population anti-passback status to a neutral status.

Z. Visitor Assignment:

1. Provide for and allow an operator to be restricted to only working with visitors. The visitor badging subsystem shall assign credentials and enroll visitors. Allow only access levels that have been designated as approved for visitors.
2. Provide an automated log of visitor name, time and doors accessed, and whom visitor contacted.
3. Allow a visitor designation to be assigned to a credential holder.
4. PACS shall be able to restrict the access levels that may be assigned to credentials that are issued to visitors.
5. Allow operator to recall visitors' credential holder file, once a visitor is enrolled in the system.
6. The operator may designate any reader as one that deactivates the credential after use at that reader. The history log shall show the return of the credential.
7. System shall have the ability to use the visitor designation in searches and reports. Reports shall be able to print all or any visitor activity.

AA. Time and Attendance:

1. Time and attendance reporting shall be provided to match IN and OUT reads and display cumulative time in for each day and cumulative time in for length of the report.

2. Shall be provided to match IN and OUT reads and display cumulative time in for each day and cumulative time in for length of the report.
3. System software setup shall allow designation of selected access-control readers as time and attendance hardware to gather the clock-in and clock-out times of the users at these readers.
   a. Reports shall show in and out times for each day, total in time for each day, and a total in time for period specified by the user.
   b. Allow the operator to view and print the reports, or save the report to a file.
   c. Alphabetically sort reports on the person's last name, by Location or location group. Include all credential holders or optionally select individual credential holders for the report.

BB. System Redundancy & High Availability: The system shall provide multiple levels of communications redundancy and failover for all PACS hosted controllers and client workstations. The PACS shall be capable of automatically re-routing communications to alternate computers across the system without operator intervention.

1. PACS system configuration with a single application/ database server shall provide at a minimum the following redundancy and failover capability:
   a. The PACS shall provide communications redundancy and failover for network-attached devices. Each network attached device shall have one or more alternative communication sever(s) that can provide hosting in case of primary communications server failure.
   b. In case of primary communications server failure, the system shall automatically re-route network-attached devices to their designated backup communications servers to allow continuous system operations without loss of alarm and event transaction processing during failover.
   c. Network-attached devices which transition to backup communications servers, shall be able to be redirected back to their default primary servers, once the primary communications servers have been restored.

CC. Tamper Protection: Tamper switches on enclosures, control units, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled. Control-station control-unit alarm display shall identify tamper alarms and indicate locations.

2.4 PACS SERVER HARDWARE

A. SMS Server Computer: Standard unmodified PC of modular design. The CPU word size shall be 64 bytes or larger; the CPU operating speed shall be at least 3.4 GHz.

1. Processor family: Intel® Xeon® E5640 (Quad Core, 2.66 GHz, 12MB L3, 80W).
2. Number of processors: 4
3. Memory: 16 GB RAM, expandable to a minimum of 192 GB without additional chassis or power supplies. Memory protection, Mirrored Memory.
4. Input/Output: 2 expansions slots, Network Controller (2) 1GbE NC382i Multifunction 4 Ports.
5. Power Supply: Dual - minimum capacity of 600 W hot plug.
6. Real-Time Clock:
   a. Accuracy: Plus or minus 1 minute per month.
   b. Time Keeping Format: 24-hour time format including seconds, minutes, hours, date, day, and month; resettable by software.
   c. Clock shall function for 1 year without power.
   d. Provide automatic time correction once every 24 hours by synchronizing clock with the Time Service Department of the U.S. Naval Observatory.
7. Serial Ports: Provide two RS-232-F serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.
8. Parallel Port: An enhanced parallel port.
9. The server shall have a 10 GB NIC or greater network card, rated at 1000/10000 MB/sec.
10. The server shall have dual 1 TB hard disk drives at 7200 RPM.
11. The server shall have a CD / DVD combo drive.
12. The server operating system shall be either (Confirm final operating system with hospital IT staff):
    a. Windows 2008 Server R2.
    b. Windows 7.
13. The Web Server shall be IIS 7.0 or better.

14. The Database shall be SQL Server 2012 (Enterprise).
15. Sound Card: For playback and recording of digital WAV sound files that are associated with audible warning and alarm functions.
16. Color Monitor: Minimum 19" or larger SVGA (1024 x 768) monitor with true color support. The server shall have a dedicated 256 MB SVGA accelerated video card with at least 64 MB onboard RAM.
17. Keyboard: With a minimum of 64 characters, standard ASCII character set based on ANSI X3.154.
18. Mouse: Standard, compatible with the installed software.
19. Special function keyboard attachments or special function keys to facilitate data input of the following operator tasks:
    a. Help.
    b. Alarm Acknowledge.
    c. Place Zone in Access.
    d. Place Zone in Secure.
    e. System Test.
    f. Print Reports.
    g. Change Operator.
20. DVD Drive:
    a. Nominal storage capacity of 4.6 GB.
21. Report Printer:
    a. Printing shall be accomplished via existing network printing system.

B. Redundant Central Computer: One identical redundant central computer, connected in a hot standby, peer configuration. This computer shall automatically maintain its own copies of system software, application software, and data files. System transactions and other activities that alter system data files shall be updated to system files of redundant computer in near real-time. If central computer fails, redundant computer shall assume control immediately and automatically.

C. PACS controllers clustering shall support the following features:
1. Assignment of Master and alternate master controllers for cluster communication to the SMS server
2. Primary and backup communication paths to the SMS server
3. Encrypted communications
4. Up to 16 controllers per cluster

5. Logical event linking between controllers in a cluster independent of SMS server communication
6. Asynchronous communication via TCP/IP (Polled devices shall not be acceptable)

2.5 STANDARD WORKSTATION HARDWARE

A. Workstation shall consist of a standard unmodified PC, with accessories and peripherals that configure the workstation for a specific duty.

B. Workstation Computer: Standard unmodified PC of modular design. The CPU word size shall be 32 bytes or larger; the CPU operating speed shall be at least 3.4 GHz.

1. Memory: 2 GB of usable installed memory, expandable to a minimum of 8 GB without additional chassis or power supplies.
2. Power Supply: Minimum capacity of 350 W.
3. Real-Time Clock:
   a. Accuracy: Plus or minus 1 minute per month.
   b. Time Keeping Format: 24-hour time format including seconds, minutes, hours, date, day, and month; resettable by software.
   c. Provide automatic time correction once every 48 hours by synchronizing clock with the Central Station.
4. Serial Ports: Provide two RS-232-F serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.
5. Parallel Port: An enhanced parallel port.
6. LAN Adapter Card: 10/100 Mbps PCI bus, internal network interface card.
7. Sound Card: For playback and recording of digital WAV sound files that are associated with audible warning and alarm functions.
8. Color Monitor: Not less than 17 inches, with a minimum resolution of 1280 by 1024] pixels, noninterlaced, and a maximum dot pitch of 0.28] mm. The video card shall support at least 256 colors at a resolution of 1280 by 1024 at a minimum refresh rate of Hz.
9. Keyboard: With a minimum of 64 characters, standard ASCII character set based on ANSI X3.154.
10. Mouse: Standard, compatible with the installed software.
11. Disk storage shall include the following, each with appropriate controller:
    a. Minimum 10 GB hard disk, maximum average access time of 10 ms.

12. DVD Drive:
    a. Nominal storage capacity of 4.6 GB.
13. Interface: Bidirectional parallel, and universal serial bus.
14. LAN Adapter Card: 10/100 Mbps internal network interface card.

2.6 CONTROLLERS

A. Controllers: Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels, and similar data downloaded from the Central Station or workstation for controlling its operation.

B. Subject to compliance with requirements in this Article, manufacturers may use multipurpose Controllers.

C. Battery Backup: Sealed, lead acid; sized to provide run time during a power outage of 90 minutes, complying with UL 924.

D. Alarm Annunciation Controller:

1. The Controller shall automatically restore communication within 10 seconds after an interruption with the field device network.
    a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.
    b. Alarm-Line Supervision:
        1) Supervise the alarm lines by monitoring each circuit for changes or disturbances in the signal, and for conditions as described in UL 1076 for line security equipment by monitoring for abnormal open, grounded, or shorted conditions using dc change measurements. System shall initiate an alarm in response to an abnormal current, which is a dc change of 5 percent or more for longer than 500 ms.
        2) Transmit alarm-line-supervision alarm to the Central Station during the next interrogation cycle after the abnormal current condition.
    c. Outputs: Managed by Central Station software.

E. Entry-Control Controller:

1. Function: Provide local entry-control functions including one- and two-way communications with access-control devices such as card readers, keypads, biometric personal identity verification devices,

door strikes, magnetic latches, gate and door operators, and exit push-buttons.

a. Operate as a stand-alone portal Controller using the downloaded database during periods of communication loss between the Controller and the field-device network.

b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:

   1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.

   2) Privileges shall include, but not be limited to, time of day control, day of week control, group control, and visitor escort control.

c. Maintain a date-, time-, and Location-stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

2. Inputs:

   a. Data from entry-control devices; use this input to change modes between access and secure.

   b. Database downloads and updates from the Central Station that include enrollment and privilege information.

3. Outputs:

   a. Indicate success or failure of attempts to use entry-control devices and make comparisons of presented information with stored identification information.

   b. Grant or deny entry by sending control signals to portal-control devices and mask intrusion alarm annunciation from sensors stimulated by authorized entries.

   c. Maintain a date-, time-, and Location-stamped record of each transaction and transmit transaction records to the Central Station.

   d. Door Prop Alarm: If a portal is held open for longer than 20 seconds, alarm sounds.

4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
5. Data Line Problems: For periods of loss of communications with Central Station, or when data transmission is degraded and generating continuous checksum errors, the Controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.
   a. Store up to 1000 transactions during periods of communication loss between the Controller and access-control devices for subsequent upload to the Central Station on restoration of communication.

2.7 PIV MIDDLEWARE

A. PIV Middleware shall provide three-factor authentication, including biometric matching using a fingerprint capture device capable of single fingerprint capture. Unit shall enable digital certificates can to be verified by security personnel using the issuer's certificate authority, SCVP, OCSP responder/repeater, or the TSA hot list for TWIC cardholders. All cards shall be validated using FIPS-201 challenge-response protocol in order to identify forged or cloned cards. PIV Middleware solution shall validate all PIV, TWIC, NG CAC, and FRAC cards. TWIC card FASC-Ns shall also be verified against a live or cached TSA hot list.

B. PIV Middleware shall have ability to:
   1. Verify cardholder identity and validates FIPS 201-compliant PIV-II, next-generation (NG) CAC, TWIC, or FRAC credentials in real-time
   2. Perform three-factor authentication of cardholder using PIN, biometrics, and certificate (or serial numbers) detecting forged or cloned cards
   3. Enroll FASC-N, photo, and pertinent cardholder information into PACS software
   4. Automatically suspend a cardholder’s badge if his or her PIV, TWIC, or CAC card certificate serial number is on the Certificate Revocation List (CRL)
   5. Upload a cardholder transaction audit trail to central database or exports it to a .csv file for centralized transaction management

6. Be compatible with biometric mobile terminal for off-site verification and enrollment
7. Re-validate imported cardholder certificates on a periodic basis via the Internet
8. Operate with commercial, off-the-shelf (COTS) FIPS 201 PIV-II and ANSI INCITS 378-compliant fingerprint capture devices
9. Revalidate imported cardholder certificates at regular intervals, ensuring that the credentials used in PACS system are backed by a valid set of digital certificates. Digital certificates are verified against local OCSP repeater/validation authority using the issuer's validation authority, or Microsoft Crypto Application Programming Interface (API) on Windows XP SP3 or Vista.
10. Certificate Manager shall fully support SCVP and OCSP for fast, online validation.
11. Provide verification of TWIC credentials against a live TSA hot list.
12. Support uploading local transactions to a central database for consolidated activity reporting. This application shall support a variety of ODBC- or ADO-compliant databases, including Oracle, SQL Server 2005, Informix, DB2, and Firebird.
13. Provide user with ability to produce canned transaction log queries as well as creating queries directly from the SQL database.

C. PIV Middleware PC requirements:

1. PIV Middleware software shall operate on Intel-based PC with minimum 1.8 GHz CPU, 1 GB RAM, 40 GB hard disk, and Microsoft Windows XP SP2 with Microsoft .NET Framework 2.0
2. Unit shall fingerprint capture devices and smart card reader.

D. PIV Middleware shall be FIPS 201 approved product.

2.8 CARD READERS

A. Power: Card reader shall be powered from its associated Controller, including its standby power source.

B. Response Time: Card reader shall respond to passage requests by generating a signal that is sent to the Controller. Response time shall be 800 ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.

C. Enclosure: Suitable for surface, semiflush, or pedestal mounting. Mounting types shall additionally be suitable for installation in the following locations:

1. Indoors, controlled environment.
2. Indoors, uncontrolled environment.
3. Outdoors, with built-in heaters or other cold-weather equipment to extend the operating temperature range as needed for operation at the site.

D. Display: LED or other type of visual indicator display shall provide visual and audible status indications and user prompts. Indicate power on/off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

E. Shall be utilized for controlling the locking hardware on a door and allows for reporting back to the main control panel with the time/date the door was accessed, the name of the person accessing the point of entry, and its location.

F. Will be fully programmable and addressable, locally and remotely, and hardwired to the system.

G. Shall be individually home run to the main panel.

H. Shall be installed in a manner that they comply with:

1. The Uniform Federal Accessibility Standards (UFAS)
2. The Americans with Disabilities Act (ADA)
3. The ADA Standards for Accessible Design

I. Shall support a variety of card readers that must encompass a wide functional range. The PACS may combine any of the card readers described below for installations requiring multiple types of card reader capability (i.e., card only, card and/or PIN, card and/or biometrics, card and/or pin and/or biometrics, supervised inputs, etc.). These card readers shall be available in the approved technology to meet FIPS 201, and is ISO 14443 A or B, ISO/IEC 7816 compliant. The reader output can be Wiegand, RS-22, 485 or TCP/IP.

J. Shall be housed in an aluminum bezel with a wide lead-in for easy card entry.

K. Shall contain read head electronics, and a sender to encode digital door control signals.

L. LED’s shall be utilized to indicate card reader status and access status.

M. Shall be able to support a user defined downloadable off-line mode of operation (e.g. locked, unlocked), which will go in effect during loss of communication with the main control panel.

N. Shall provide audible feedback to indicate access granted/denied decisions. Upon a card swipe, two audible tones or beeps shall indicate access granted and three tones or beeps shall indicate access denied. All keypad buttons shall provide tactile audible feedback.

O. Shall have a minimum of two programmable inputs and two programmable outputs.

P. **ALTERNATE BID NO. PACS-2 – All c**ard readers that utilize scramble pad controls, for secondary authentication, along with a proximity reader shall meet the following specifications:

1. Entry control keypads shall use be scramble pad type requiring a unique combination of alphanumeric and other symbols as an identifier. Scramble pads shall contain an integral, randomly generated, alphanumeric/special symbols keyboard. Communications protocol shall be compatible with the local processor.
2. Each PIN access code issued shall be unique, no two user shall receive the same access code.

Q. Shall include a Light Emitting Diode (LED) or other type of visual indicator display and provide visual or visual and audible status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected. The design of the keypad display or keypad enclosure shall limit the maximum horizontal and vertical viewing angles of the keypad. The maximum horizontal viewing angle shall be plus and minus five (5) degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display. The maximum vertical viewing angle shall be plus and minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.

1. Shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 milliseconds or less from the time the last alphanumeric symbol is entered until a response signal is generated.
2. Shall be powered from the source as designed and shall not dissipate more than 150 Watts.

3. Shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.
4. Shall provide a means for users to indicate a duress situation by entering a special code.

R. PIV Contact Card Reader

1. Application Protocol Data Unit (APDU) Support: At a minimum, the contact interface shall support all card commands for contact based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.
2. Buffer Size: The reader must contain a buffer large enough to receive the maximum size frame permitted by International Organization for Standardization International Electrotechnical Commission (ISO/IEC) 7816-3:1997, Section 9.4.
3. Programming Voltage: PIV Readers shall not generate a Programming Voltage.
4. Support for Operating Class: PIV Readers shall support cards with Class A Vccs as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.
5. Retrieval Time: Retrieval time for 12.5 kilobytes (KB) of data through the contact interface of the reader shall not exceed 2.0 seconds.
6. Transmission Protocol: The PIV Reader shall support both the character-based T=0 protocol and block-based T=1 protocol as defined in ISO/IEC 7816-3:1997.
7. Support for PPS Procedure: The reader shall support Protocol and Parameters Selection (PPS) procedure by having the ability to read character TA1 of the Answer to Reset (ATR) sent by the card as defined in ISO/IEC 7816-3:1997.

2.9 BIOMETRIC IDENTITY VERIFICATION EQUIPMENT

A. Shall be FIPS 201 and NIST SP 800-76 compliant.

B. Shall utilize fingerprint verification.

C. Shall be programmable, addressable, and hardwired directly to the main control panel. Shall be either daisy chained or individually home run to the main control panel.

D. Shall be installed in a manner that they comply with:

1. The Uniform Federal Accessibility Standards (UFAS)

2. The Americans with Disabilities Act (ADA)
3. The ADA Standards for Accessible Design

E. Shall include a means to construct individual templates or profiles based upon measurements taken from the person to be enrolled. This template shall be stored as part of the System Reference Database Files. The stored template shall be used as a comparative base by the personnel identity verification equipment to generate appropriate signals to the associated local processors.

F. Shall interface with PACS and SMS and provide the employee’s name, contact information, and point of access.

G. Shall allow for surface, flush, or pedestal mounting.

H. Shall have communications protocol in place that shall allow for communications with the SMS.

I. Shall determine when multiple attempts were made for verification, and shall automatically prompt the user for additional attempts up to a maximum of three tries. After a third failed attempt the unit shall generate an entry control alarm. This alarm will report to the SMS and, if applicable, the CCTV system. The camera viewpoint for where the alarm was generated shall automatically be called up onto a monitor and be recorded via the recording equipment. An alarm within the SMS shall also be generated recording, at a minimum, the date, time, and attempted point of entry.

J. Fingerprint Verification:

1. Shall use a unique human fingerprint pattern to identify authorized, enrolled personnel.
2. Shall allow the user’s hand to remain in full view during the scanning process, shall incorporate positive measures to establish that the hand or fingers being scanned by the device belong to a living human being.
3. Shall provide an optical or other type of scan of the user’s fingers. The fingerprint verification scanner shall automatically initiate the scan process provided the user’s fingers are positioned.
4. LED or other type of visual indicator displays shall provide a visual or visual and audible status indication and enrollee prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected.

5. Any significant change to the user’s finger such as scars, loss of digit, or any other change that will alter the finger print shall require an update to the unit and SMS.
6. Shall provide an adjustable acceptance tolerance or template match criteria under system manager/operator control.
7. Shall respond to passage requests by generating signals to the local processor. The verification time shall be 2.0 seconds or less from the moment the finger print analysis scanner initiates the scan process until the fingerprint analysis scanner generates a response signal.
8. Shall:
   a. Provide an enrollment mode, recognition mode, and code/credential verification mode. The enrollment mode shall create a fingerprint template for new personnel and enter the template into the system database file created for that person.
   b. Template information shall be compatible with the system application software.
   c. The operating mode shall be selectable by the system manager/operator from the central station.
9. When operating in recognition mode, the fingerprint analysis scanner shall allow passage when the fingerprint data from the verification attempt matches a fingerprint template stored in the database files.
10. When operating in code/credential verification mode, the fingerprint analysis scanner shall allow passage when the fingerprint data from the verification attempt matches a fingerprint template associated with the identification code. When entered into a keypad or it matches the fingerprint template associated with credential, the card data will then be recognized by the card reader.
11. Shall store template transactions involving fingerprint scans. The template match scores shall be stored in the matching personnel data file in a format compatible with the system application software, and shall be used for report generation.
12. Shall be unit listed as FIPS 201 Approved product.

2.10 CREDENTIAL CARDS

A. Personal Identity Verification (PIV) credential cards shall comply to Federal Information Processing Standards Publication (FIPS) 201.
B. Visual Card Topography shall be compliant with NIST 800-104.

C. PIV logical credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels. These mandatory data elements shall collectively comprise the data model for PIV logical credentials, and include the following:

   1. CHUID
   2. PIN
   3. PIV authentication data (one asymmetric key pair and corresponding certificate)
   4. Two biometric fingerprints, if cardholder's security clearance will require secondary authentication.

D. The credential card (PIV) shall be an ISO 14443 type smart card with contactless interface that operates at 13.56 MHZ.

E. Coordinate with Hospital on exact type of card that shall be provided, default style of PIV card shall be an ISO 7816 type smart card.

2.11 SYSTEM SENSORS AND RELATED EQUIPMENT

A. The PACS (Physical Access Control System) and related Equipment provided by the Contractor shall meet or exceed the following performer specifications:

B. Door Status Indicators:

   1. Shall monitor and report door status to the SMS.
   2. Door Position Sensor (door contact):
      a. Shall provide an open or closed indication for all doors operated on the PACS and report directly to the SMS.
      b. Shall also provide alarm input to the Intrusion Detection System for all doors operated by the PACS and all other doors that require monitoring by the intrusion detection system.
      c. Switches for doors operated by the PACS shall be double pole double throw (DPDT). One side of the switch shall monitor door position and the other side if the switch shall report to the intrusion detection system. For doors with electromagnetic locks a magnetic bonding sensor (MBS) can be used in place of one side of a DPDT switch, in turn allowing for the use of a single pole double throw (SPDT) switch in its place of a DPDT switch.
      d. Switches for doors not operated by the PACS shall be SPDT and report directly to the IDS.
      e. Shall be surface or flush mounted and wide gap with the ability to operate at a maximum distance of up to 2” (5 cm).

2.12 PUSH BUTTON SWITCHES

A. Push-Button Switches: Momentary-contact back-lighted push buttons, with stainless-steel switch enclosures.

1. Electrical Ratings:

a. Minimum continuous current rating of 10 A at 120 V.

b. Contacts that will make 720 VA at 60 A and that will break at 720 VA at 10 A.

2. Enclosures: Flush or surface mounting. Push buttons shall be suitable for flush mounting in the switch enclosures.

3. Enclosures shall additionally be suitable for installation in the following locations:

a. Indoors, controlled environment.

b. Indoors, uncontrolled environment.

c. Outdoors.

4. Power: Push-button switches shall be powered from their associated Controller, using dc control.

2.13 INTERFACES

A. CCTV System Interface – If Applicable

1. An RS232 or Ethernet interface associated driver, and controller shall be provided for connection of the SMS Central Computer to the CCTV Alarm interface and switcher. The interface shall provide alarm data to the CCTV Alarm interface for automatic camera call-up. If required the Security Contractor shall be responsible for programming the command strings into the SMS Server.

B. Power Supplies:

1. Four (4) Amp DC Power Supply:

a. Power supply shall be Class 2 rated and be UL 294 and 1076 listed provided in grey, lockable enclosure, suited for wall mounting applications.

b. Switch selectable 12 VDC or 24VDC power limited output.

c. Input of 115 VAC, 60 Hz, 1.45A with maximum charge current of 0.7A.

d. Output shall be filtered and electronically regulated.

1) 4 maps continuous supply current at 12 VDC.

2) 3 amps continuous supply current at 24 VDC.

e. Built-in charger for sealed lead acid batteries, two (2) 12 Amp-Hour batteries (minimum capacity). Automatic switchover to standby batteries when AC input fails.

f. Complete with form C contacts for supervision functions.

g. Thermal overload and short circuit protection.

h. The power supply shall be provided with:

1) Tamper switch.

2) 16 standoffs and 16 screws.

3) Provisions for mounting two PACS system controllers within enclosure.

2. Six (6) Amp DC Power Supply:

a. Power supply shall be Class 2 rated and be UL 294 and 1076 listed provided in grey, lockable enclosure, suited for wall mounting applications.

b. Switch selectable 12 VDC or 24VDC power limited output.

c. Input of 115 VAC, 60 Hz, 1.9A with maximum charge current of 0.7A.

d. Output shall be filtered and electronically regulated, with maximum 100mV peak output voltage ripple.

1) 6 maps continuous supply current at 12 or 24 VDC.

e. Four individual, surge protected, circuit breaker outputs.

e. Built-in charger for sealed lead acid batteries, two (2) 7 Amp-Hour batteries (minimum capacity). Automatic switchover to standby batteries when AC input fails.

f. Complete with form C contacts for supervision functions.

g. Thermal overload and short circuit protection.

h. The power supply shall be provided with:

1) Tamper switch.

2) 48 standoffs and 48 screws.

3) Provisions for mounting six PACS system controllers within enclosure.

2.14 VIDEO AND CAMERA CONTROL – IF APPLICABLE

A. Control station or designated workstation displays live video from a CCTV source.

1. Control Buttons: On the display window, with separate control buttons to represent Left, Right, Up, Down, Zoom In, Zoom Out, Scan, and a minimum of two custom command auxiliary controls.

2. Provide at least seven icons to represent different types of cameras, with ability to import custom icons. Provide option for display of icons on graphic maps to represent their physical location.
3. Provide the alarm-handling window with a command button that will display the camera associated with the alarm point.

B. Display mouse-selectable icons representing each camera source, to select source to be displayed. For CCTV sources that are connected to a video switcher, control station shall automatically send control commands through a COM port to display the requested camera when the camera icon is selected.

C. Allow cameras with preset positioning to be defined by displaying a different icon for each of the presets. Provide control with Next and Previous buttons to allow operator to cycle quickly through the preset positions.

2.15 WIRES AND CABLES

A. Comply with Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY."

B. Plenum-Type, RS-232 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, and individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage; plastic jacket. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

C. Plenum-Type, RS-485 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and fluorinated-ethylene-propylene jacket.
1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

D. Plenum-Type, Paired, Reader Cable: Paired, 3 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, individual aluminum foil-polypropylene tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and fluorinated-ethylene-propylene jacket.
1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

E. Plenum-Type, Multiconductor, Reader Cable: 6 conductors, No. 20 AWG, stranded (7x28) tinned copper conductors, fluorinated-ethylene-propylene insulation, overall aluminum foil-polyester tape shield with 100 percent shield coverage plus tinned copper braid shield with 85 percent shield coverage, and fluorinated-ethylene-propylene jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

F. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

G. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

H. Plenum-Type, Paired Input Cable: 1 pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, aluminum foil-polyester tape shield (foil side out), with No. 22 AWG drain wire, 100 percent shield coverage, and plastic jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

I. Plenum-Type, Paired AC Transformer Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

J. LAN (Ethernet) Cabling: Comply with Division 28 Section "Conductors and Cables for Electronic Safety and Security."

PART 3 - EXECUTION

3.1 GENERAL

A. The Contractor shall install all system components and appurtenances in accordance with the manufacturers' instructions, ANSI C2, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified. Control signals, communications, and data transmission lines grounding shall be installed as necessary to preclude ground loops, noise, and surges from affecting system operation. Equipment, materials, installation, workmanship, inspection, and testing shall be in accordance with manufacturers' recommendations and as modified herein.

B. Consult the manufacturers' installation manuals for all wiring diagrams, schematics, physical equipment sizes, etc., before beginning system installation. Refer to the Riser/Connection diagram for all schematic system installation/termination/wiring data.

C. All equipment shall be attached to walls and ceiling/floor assemblies and shall be held firmly in place (e.g., sensors shall not be supported solely by suspended ceilings). Fasteners and supports shall be adequate to support the required load.

3.2 CURRENT SITE CONDITIONS

A. After contract is awarded, Contractor shall visit the site and verify that site conditions are in agreement with the design package. The Contractor shall report all changes to the site or conditions which will affect performance of the system to the Owner in a report as defined in paragraph Group II Technical Data Package. The Contractor shall not take any corrective action without written permission from the Owner.

3.3 EXAMINATION

A. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

B. Examine roughing-in for LAN and control cable conduit systems to PCs, Controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.4 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."

C. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.

1. Record setup data for control station and workstations.
2. For each Location, record setup of Controller features and access requirements.
3. Propose start and stop times for time zones and holidays, and match up access levels for doors.
4. Set up groups, linking, and list inputs and outputs for each Controller.
5. Assign action message names and compose messages.
6. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
7. Prepare and install alarm graphic maps.
8. Develop user-defined fields.
9. Develop screen layout formats.
10. Propose setups for guard tours and key control.
11. Discuss badge layout options; design badges.
12. Complete system diagnostics and operation verification.
13. Prepare a specific plan for system testing, startup, and demonstration.
14. Develop acceptance test concept and, on approval, develop specifics of the test.
15. Develop cable and asset management system details; input data from construction documents. Include system schematics and Technical Drawings.

D. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

3.5 CABLING

A. Comply with NECA 1, "Good Workmanship in Electrical Contracting."

B. Install cables and wiring according to requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."

C. Wiring Method: Install wiring in raceway within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces. Fish multi-conductor cable through existing construction where cutting of the wall is not feasible. If concealment of raceway is not possible, the use of surface metal raceway shall be considered, contractor shall submit samples of raceway for approval to hospital and architect. Contractor is responsible for all patching and painting if required due to installation of PACS equipment.

D. Install LAN cables using techniques, practices, and methods that are consistent with Category 6 rating of components and that ensure Category 5E performance of completed and linked signal paths, end to end.

E. Install cables without damaging conductors, shield, or jacket.

F. Boxes and enclosures containing security system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Boxes above ceiling level in occupied areas of the building shall not be considered to be accessible. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.

G. Install end-of-line resistors at the field device location and not at the Controller or panel location.

3.6 CABLE APPLICATION

A. Comply with EIA/TIA-569, "Commercial Building Standard for Telecommunications Pathways and Spaces."

B. Cable application requirements are minimum requirements and shall be exceeded if recommended or required by manufacturer of system hardware.

C. RS-232 Cabling: Install at a maximum distance of 50 feet (15 m).

D. RS-485 Cabling: Install at a maximum distance of 4000 feet.

E. Card Readers:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from Controller to the reader is 250 feet, and install No. 20 AWG wire if maximum distance is 500 feet.
3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the Controller.
4. Install minimum No. 18 AWG shielded cable to readers that draw 50 mA or more.

F. Install minimum No. 16 AWG cable from Controller to electrically powered locks. Do not exceed 250 feet.

G. Install minimum No. 16 AWG ac power wire from transformer to Controller.

3.7 GROUNDING

A. Comply with Division 26 Section "Grounding and Bonding for Electrical Systems."

B. Comply with IEEE 1100, "Power and Grounding Sensitive Electronic Equipment."

C. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

D. Signal Ground:

1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.
2. Bus: Provide grounding bus with equipment enclosures, provide with standoff insulators to isolate bus from equipment enclosure.
3. Backbone Cable: Extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

3.8 INSTALLATION

A. System installation shall be in accordance with UL 294, manufacturer and related documents and references, for each type of security subsystem designed, engineered and installed.

B. Components shall be configured with appropriate “service points” to pinpoint system trouble in less than 30 minutes.

C. The Contractor shall install all system components including Government furnished equipment, and appurtenances in accordance with the manufacturer's instructions, documentation listed in Sections 1.4 and 1.5 of this document, and shall furnish all necessary connectors, terminators, interconnections, services, and adjustments required for a operable system.

D. The PACS will be designed, engineered, installed, and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the system is a stand alone or a network.

E. For integration purposes, the PACS shall be integrated where appropriate with the following associated security subsystems:

1. CCTV:

a. Be able to monitor, control and record cameras on a 24 hours basis.

b. Be programmed automatically call up a camera when an access point is but into an alarm state.

c. For additional PACS system requirements as they relate to the CCTV, refer to Section 28 23 00, VIDEO SURVEILLANCE.

F. Integration with these security subsystems shall be achieved by computer programming or the direct hardwiring of the systems.

G. For programming purposes refer to the manufacturers requirements for correct system operations. Ensure computers being utilized for system integration meet or exceed the minimum system requirements outlined on the systems software packages.

H. The Contractor shall visit the site and verify that site conditions are in agreement with the design package. The Contractor shall report all changes to the site or conditions that will affect performance of the system. The Contractor shall not take any corrective action without written permission from the Government.

I. The Contractor shall visit the site and verify that site conditions are in agreement/compliance with the design package. The Contractor shall report all changes to the site or conditions that will affect performance of the system to the Contracting Officer in the form of a report. The Contractor shall not take any corrective action without written permission received from the Contracting Officer.

J. Existing Equipment:

1. The Contractor shall connect to and utilize existing door equipment, control signal transmission lines, and devices as outlined in the design package. Door equipment and signal lines that are usable in their original configuration without modification may be reused with Contracting Officer approval.

2. The Contractor shall perform a field survey, including testing and inspection of all existing door equipment and signal lines intended to be incorporated into the PACS, and furnish a report to the Contracting Officer as part of the site survey report. For those items considered nonfunctioning, provide (with the report) specification sheets, or written functional requirements to support the findings and the estimated cost to correct the deficiency. As

part of the report, the Contractor shall include a schedule for connection to all existing equipment.

3. The Contractor shall make written requests and obtain approval prior to disconnecting any signal lines and equipment, and creating equipment downtime. Such work shall proceed only after receiving Contracting Officer approval of these requests. If any device fails after the Contractor has commenced work on that device, signal or control line, the Contractor shall diagnose the failure and perform any necessary corrections to the equipment.
4. The Contractor shall be held responsible for repair costs due to Contractor negligence, abuse, or improper installation of equipment.
5. The Contracting Officer shall be provided a full list of all equipment that is to be removed or replaced by the Contractor, to include description and serial/manufacturer numbers where possible. The Contractor shall dispose of all equipment that has been removed or replaced based upon approval of the Contracting Officer after reviewing the equipment removal list. In all areas where equipment is removed or replaced the Contractor shall repair those areas to match the current existing conditions.

K. Enclosure Penetrations: All enclosure penetrations shall be from the bottom of the enclosure unless the system design requires penetrations from other directions. Penetrations of interior enclosures involving transitions of conduit from interior to exterior, and all penetrations on exterior enclosures shall be sealed with rubber silicone sealant to preclude the entry of water and will comply with VA Master Specification 07 84 00, Firestopping. The conduit riser shall terminate in a hot-dipped galvanized metal cable terminator. The terminator shall be filled with an approved sealant as recommended by the cable manufacturer and in such a manner that the cable is not damaged.

L. Cold Galvanizing: All field welds and brazing on factory galvanized boxes, enclosures, and conduits shall be coated with a cold galvanized paint containing at least 95 percent zinc by weight.

M. Control Panels:

1. Connect power and signal lines to the controller.
2. Program the panel as outlined by the design and per the manufacturer’s programming guidelines.

N. SMS:

1. Coordinate with the VA agency’s IT personnel to place the computer on the local LAN or Intranet and provide the security system protection levels required to insure only authorized VA personnel have access to the system.
2. Program and set-up the SMS to ensure it is in fully operation.

O. Card Readers:

1. Connect all signal inputs and outputs as shown and specified.
2. Terminate input signals as required.
3. Program and address the reader as per the design package.
4. Readers shall be surface or flushed mounted and all appropriate hardware shall be provided to ensure the unit is installed in an enclosed conduit system.

P. Biometrics:

1. Connect all signal input and output cables along with all power cables.
2. Program and ensure the device is in operating order.

Q. Portal Control Devices:

1. Install all signal input and output cables as well as all power cables.
2. Devices shall be surface or flush mounted as per the design package.
3. Program all devices and ensure they are working.

R. Door Status Indicators:

1. Install all signal input and output cables as well as all power cables.
2. RTE’s shall be surface mounted and angled in a manner that they cannot be compromised from the non-secure side of a windowed door, or allow for easy release of the locking device from a distance no greater than 6 feet from the base of the door.
3. Door position sensors shall be surface or flush mounted and wide gap with the ability to operate at a maximum distance of up to 2”.

S. Entry Control Devices:

1. Install all signal input and power cables.
2. Strikes and bolts shall be mounted within the door frame.
3. Mortise locks shall be mounted within the door and an electric transfer hinge shall be utilized to transfer the wire from within the door frame to the mortise lock inside the door.

4. Electromagnetic locks shall be installed with the mag-lock mounted to the door frame and the metal plate mounted to the door.

T. System Start-Up:

1. The Contractor shall not apply power to the PACS until the following items have been completed:
   a. PACS equipment items and have been set up in accordance with manufacturer's instructions.
   b. A visual inspection of the PACS has been conducted to ensure that defective equipment items have not been installed and that there are no loose connections.
   c. System wiring has been tested and verified as correctly connected as indicated.
   d. All system grounding and transient protection systems have been verified as installed and connected as indicated.
   e. Power supplies to be connected to the PACS have been verified as the correct voltage, phasing, and frequency as indicated.
2. Satisfaction of the above requirements shall not relieve the Contractor of responsibility for incorrect installation, defective equipment items, or collateral damage as a result of Contractor work efforts.
3. The Commissioning Agent will observe startup and contractor testing of selected equipment. Coordinate the startup and contractor testing schedules with the COR and Commissioning Agent. Provide a minimum of 7 days prior notice.

U. Supplemental Contractor Quality Control:

1. The Contractor shall provide the services of technical representatives who are familiar with all components and installation procedures of the installed PACS; and are approved by the Contracting Officer.
2. The Contractor will be present on the job site during the preparatory and initial phases of quality control to provide technical assistance.
3. The Contractor shall also be available on an as needed basis to provide assistance with follow-up phases of quality control.
4. The Contractor shall participate in the testing and validation of the system and shall provide certification that the system installed

is fully operational as all construction document requirements have been fulfilled.

3.9 SYSTEM SOFTWARE

A. Install, configure, and test software and databases for the complete and proper operation of systems involved. Assign software license to Owner. Train owner or owners representative on software functionality.

3.10 FIELD QUALITY CONTROL

A. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect, test, and adjust field-assembled components and equipment installation, including connections, and to assist in field testing. Report results in writing.

B. Testing Agency: Engage a qualified testing and inspecting agency to perform field tests and inspections and prepare test reports:

C. Perform the following field tests and inspections and prepare test reports:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1, "Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA-568-B.
2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

3.11 PROTECTION

A. Maintain strict security during the installation of equipment and software. Rooms housing the control station, and workstations that have been powered up shall be locked and secured, with an activated burglar alarm and access-control system reporting to a Central Station complying with UL 1610, "Central-Station Burglar-Alarm Units," during periods when a qualified operator in the employ of Contractor is not present.

3.12 COMMISSIONING

A. Provide commissioning documentation in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS for all inspection, start up, and contractor testing required above and required by the System Readiness Checklist provided by the Commissioning Agent.

B. Components provided under this section of the specification will be tested as part of a larger system. Refer to Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS and related sections for contractor responsibilities for system commissioning.

3.13 DEMONSTRATION AND TRAINING

A. Provide services of manufacturer’s technical representative for four hours to instruct VA personnel in operation and maintenance of units.

B. Submit training plans and instructor qualifications in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

C. Develop separate training modules for the following:

1. Computer system administration personnel to manage and repair the LAN and databases and to update and maintain software.
2. Operators who prepare and input credentials to man the control station and workstations and to enroll personnel.
3. Security personnel.
4. Hardware maintenance personnel.
5. Corporate management.

D. All testing and training shall be compliant with the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.

-----END----

SECTION 28 13 16
PHYSICAL ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT

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

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 26 05 33 – RACEWAYS AND BOXES FOR ELECTRICAL SYSTEMS. Requirements for infrastructure.

D. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.

E. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.

F. Section 28 08 00 - COMMISIONING 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 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

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 an 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 eight hours of receipt of notification that service is needed. Submit name and address of service organizations.

1.4 SUBMITTALS

A. Provide certificates of compliance with Section 1.3, Quality Assurance.

B. Provide submittal along with submittals required by section 28 13 00, conforming to all requirements of said section.

1.5 APPLICABLE PUBLICATIONS

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):

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. National Electrical Contractors Association

303-2005................Installing Closed Circuit Television (CCTV) Systems

F. National Electrical Manufactures Association (NEMA):

250-08..................Enclosures for Electrical Equipment (1000 Volts Maximum)

G. National Fire Protection Association (NFPA):

70-11................... National Electrical Code

H. Underwriters Laboratories, Inc. (UL):

294-99..................The Standard of Safety for Access Control System Units

I. Homeland Security Presidential Directive (HSPD):

HSPD-12.................Policy for a Common Identification Standard for Federal Employees and Contractors

J. Federal Information Processing Standards (FIPS):

FIPS-201-1..............Personal Identity Verification (PIV) of Federal Employees and Contractors

K. 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)

L. 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

M. Uniform Federal Accessibility Standards (UFAS) 1984

N. 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

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] 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, Existing database files. 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 individual system operators, each with a unique password.
2. Operator Password: Eight alphanumeric characters
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 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.

H. Access Card/Code Operation and Management: Access authorization shall be a combination of either card, by a manually entered code (PIN), or 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.
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 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 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 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 Service 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

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----

SECTION 28 23 00
VIDEO SURVEILLANCE

PART 1 – GENERAL

1.1 DESCRIPTION

A. Provide and install a complete Video Surveillance System, which is identified as the Video Assessment and Surveillance System hereinafter referred to as the VASS System as specified in this section.

B. This Section includes video surveillance system consisting of cameras, data transmission wiring, and a control station with its associated equipment.

C. Video surveillance system Video assessment & surveillance system shall be integrated with monitoring and control system specified in Division 28 Section PHYSICAL ACCESS CONTROL that specifies systems integration.

1.2 RELATED WORK

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.

C. Section 10 14 00 - SIGNAGE. Requirements for labeling and signs.

D. Section 26 05 11 - REQUIREMENTS FOR ELECTRICAL INSTALLATIONS. Requirements for connection of high voltage.

E. Section 26 05 21 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES (600 VOLTS AND BELOW). Requirements for power cables.

F. Section 26 05 41 - UNDERGROUND ELECTRICAL CONSTRUCTION. Requirements for underground installation of wiring.

G. 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.

H. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.

I. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.

J. Section 28 05 28.33 - CONDUITS AND BACKBOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.

K. Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY. Requirements for commissioning, systems readiness checklists, and training.

L. Section 28 13 00 - PHYSICAL ACCESS CONTROL SYSTEM. Requirements for physical access control system integration.

1.3 DEFINITIONS

A. AGC: Automatic gain control.

B. B/W: Black and white.

C. CCD: Charge-coupled device.

D. CIF: Common Intermediate Format CIF images are 352 pixels wide and 240 (NTSC) pixels tall (352 x 240).

E. 4CIF: resolution is 704 pixels wide and 480 (NTSC) pixels tall (704 x 480).

F. H.264 (also known as MPEG4 Part 10): an encoding format that compresses video much more effectively than older (MPEG4) standards.

G. ips: Images per second.

H. MPEG: Moving picture experts group.

I. MPEG4: a video encoding and compression standard that uses inter-frame encoding to significantly reduce the size of the video stream being transmitted.

J. NTSC: National Television System Committee.

K. UPS: Uninterruptible power supply.

L. PTZ: refers to a movable camera that has the ability to pan left and right, tilt up and down, and zoom or magnify a scene.

1.4 QUALITY ASSURANCE

A. The Contractor shall be responsible for providing, installing, and the operation of the VASS System 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 complete 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. Manufacturers Qualifications: The manufacturer shall regularly and presently produce, as one of the manufacturer's principal products, the equipment and material specified for this project, and shall have manufactured the item for at least three years.

E. Product Qualification:

1. Manufacturer's product shall have been in satisfactory operation, on three installations of similar size and type as this project, for approximately three years.
2. The Government reserves the right to require the Contractor to submit a list of installations where the products have been in operation before approval.

F. Contractor Qualification:

1. The Contractor or security sub-contractor shall be a licensed security Contractor with a minimum of five (5) years' experience installing and servicing systems of similar scope and complexity. The Contractor shall be an authorized regional representative of the Video Assessment and Surveillance System’s (VASS) manufacturer. The Contractor shall provide four (4) current references from clients with systems of similar scope and complexity which became operational in the past three (3) years. At least three (3) of the references shall be utilizing the same system components, in a similar configuration as the proposed system. The references must include a current point of contact, company or agency name, address, telephone number, complete system description, date of completion, and approximate cost of the project. The owner reserves the option to visit the reference sites, with the site owner’s permission and representative, to verify the quality of installation and the references’ level of satisfaction with the system. The Contractor shall provide copies of system manufacturer certification for all technicians. The Contractor shall only utilize factory-trained technicians to install, program, and service the VASS. The Contractor shall only utilize factory-trained technicians to install, terminate and service cameras, control, and recording equipment. The technicians shall have a minimum of five (5) continuous years of technical experience in electronic security systems. The Contractor shall have a local service facility. The facility shall be located within 60 miles of the project site. The local facility shall include sufficient spare parts inventory to support the service requirements associated with this contract. The facility shall also include appropriate diagnostic equipment to perform diagnostic procedures. The COTR reserves the option of

surveying the company’s facility to verify the service inventory and presence of a local service organization.

2. The Contractor shall provide proof project superintendent with BICSI Certified Commercial Installer Level 1, Level 2, or Technician to provide oversight of the project.
3. Cable installer must have on staff a Registered Communication Distribution Designer (RCDD) certified by Building Industry Consulting Service International. The staff member shall provide consistent oversight of the project cabling throughout design, layout, installation, termination and testing.

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

1.5 SUBMITTALS

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 Drawings.

B. Provide certificates of compliance with Section 1.4, Quality Assurance.

C. Provide a pre-installation and as-built design package in both electronic format and on paper, minimum size 1220 x 1220 millimeters (48 x 48 inches); 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. Floor plans, site plans, and enlarged 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 VASS 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 clearly defined and 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 the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.

H. Submit completed System Readiness Checklists provided by the Commissioning Agent and completed by the contractor, signed by a qualified technician and dated on the date of completion, in accordance with the requirements of Section 28 08 00 COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

1.6 APPLICABLE PUBLICATIONS

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)/Electronic Industries Alliance (EIA):

330-09..................Electrical Performance Standards for CCTV Cameras

375A-76.................Electrical Performance Standards for CCTV Monitors

C. Institute of Electrical and Electronics Engineers (IEEE):

C62.41-02...............IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits

802.3af-08..............Power over Ethernet Standard

D. Federal Communications Commission (FCC):

(47 CFR 15) Part 15.... Limitations on the Use of Wireless Equipment/Systems

E. National Electrical Contractors Association (NECA):

303-2005................Installing Closed Circuit Television (CCTV) Systems

F. National Fire Protection Association (NFPA):

70-08...................Article 780-National Electrical Code

G. Federal Information Processing Standard (FIPS):

140-2-02................Security Requirements for Cryptographic Modules

H. Underwriters Laboratories, Inc. (UL):

983-06..................Standard for Surveillance Camera Units

3044-01.................Standard for Surveillance Closed Circuit Television Equipment

1.7 COORDINATION

A. Coordinate arrangement, mounting, and support of video surveillance equipment:

1. To allow maximum possible headroom unless specific mounting heights that reduce headroom are indicated.
2. To provide for ease of disconnecting the equipment with minimum interference to other installations.

3. To allow right of way for piping and conduit installed at required slope.
4. So connecting raceways, cables, wireways, cable trays, and busways will be clear of obstructions and of the working and access space of other equipment.

B. Coordinate installation of required supporting devices and set sleeves in cast-in-place concrete, masonry walls, and other structural components as they are constructed.

C. Coordinate location of access panels and doors for video surveillance items that are behind finished surfaces or otherwise concealed.

1.8 WARRANTY OF CONSTRUCTION

A. Warrant VASS System work subject to the Article “Warranty of Construction” of FAR clause 52.246-21.

B. Demonstration and training shall be performed prior to system acceptance.

PART 2 – PRODUCTS

2.1 MANUFACTURES

A. Basis-of-Design Product: Subject to compliance with requirements, provide product indicated on the Contract Drawings from Pelco or comparable product by one of the following:

1. Pelco by Schneider Electric.
2. Bosch Security Systems, Inc.
3. Vicon.

2.2 GENERAL

A. Video signal format shall comply with the NTSC standard Internet Protocol (IP).

B. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor entry connection to components.

C. Power Connections: Comply with requirements in Section 28 05 00 COMMON WORK REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY, Part 2, as recommended by manufacturer for type of line being protected.

D. Tamper Protection: Tamper switches on enclosures, control units, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled. Control-station, control-unit alarm display shall identify tamper alarms and indicate locations.

2.3 CAMERAS

A. All Cameras will be EIA 330 and UL 1.Minimum Protection for Power Connections 120 V and more: Auxiliary panel suppressors shall comply with requirements in Section 28 05 00 COMMON WORK REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY, Part 2.

B. Minimum Protection for Communication, Signal, Control, and Low-Voltage 983 compliant as well as:

1. Will be charge coupled device (CCD cameras and shall conform to National Television System Committee (NTSC) formatting.
2. Fixed cameras shall be color and the primary choice for monitoring following the activities described below. Pan/Tilt/Zoom (P/T/Z) cameras shall be color and are to be utilized to complement the fixed cameras.
3. P/T/Z cameras shall be powered by 24 volts direct current (VDC) or 24 volts alternate current (VAC). Power supplies shall be Class 2 and UL compliant and have a back-up power source to ensure cameras are still operational in the event of loss of primary power to the VASS System.
4. Building Interior fixed cameras shall be powered over Ethernet. Network switches supporting PoE cameras shall have a back-up power source to ensure cameras are still operational in the event of loss of primary power to the VASS System.
5. Shall be rated for continuous operation under the environmental conditions listed in Part 1, Project Conditions.
6. Will be home run to an Ethernet switch and monitored on a 24 hour basis at a designated Security Management System location.
7. Each function and activity shall be addressed within the system by a unique user defined name, with minimum of twenty (20) characters. The use of codes or mnemonics identifying the VASS action shall not be accepted.
8. Shall come with built-in video motion detection that shall automatically monitor and process information from each camera. The camera motion detection shall detect motion within the camera's field of view and provide automatic visual, remote alarms as a result of detected motion.

9. Shall be programmed to digitally flip from color to black and white at dusk and at low light conditions.
10. P/T/Z cameras shall be utilized in a manner that they complement fixed cameras and shall not be used as a primary means of monitoring activity.
11. Dummy or fake cameras will not be utilized at any time.
12. Appropriate signage shall be designed, provided, and posted that notifies people that an area is under camera surveillance.

2.4 VIDEO MANAGEMENT SYSTEM (ANALOG)

A. Video distribution amplifier shall be model VDA-412 as manufactured by Compu-Video Systems, or approved equal. The video distribution amplifier shall be (4) 1x2 channel "cascadable" array with each input provided with two outputs. Provide high quality Color video performance. Input and output connectors shall be Composite Video BNC. Input and output impedance shall be 75 ohm +/-5 percent. Frequency response 0-60mHz +/-.5dB. Horizontal and Vertical Tilt shall each be less than 1 percent. Differential gain shall be less than 1 percent. Differential phase shall be less than 1 degree. 12VDC power source with 120V adapter. Provide all required hardware to wall mount the unit. The unit shall operate using 120V AC-60Hz

B. IP Network Video Encoder

1. The video encoder shall be standards-compliant and provide a fully supported API that shall integrate with multiple video management systems.
2. The video encoder shall support 4 camera inputs.
3. The 4-input encoder shall be powered by a 12VDC source.
4. The video encoder shall generate compressed H.264 video streams in standards-compliant baseline profile, main profile, or high profile. For 4CIF resolution, the encoder shall employ de-interlacing technology to support interlaced cameras while remaining compatible with standards-based decoders at baseline profile.
5. The video encoder shall provide for two independently configurable streams for each camera input. Each stream shall be capable of 4CIF resolution, 30 or 25 images per second (ips), NTSC or PAL. The settings of one stream shall not interfere or limit the settings for the second stream.

6. The video encoder shall be capable of generating 4CIF resolution, real-time video streams while also running intelligent video content analysis algorithms on each camera input. There shall be no need to degrade video resolution or frame rate to execute analytics algorithms.
7. The video encoder shall provide support for running any three video content analysis algorithms simultaneously on each channel. In addition, the encoder shall also be capable of processing video content analysis algorithms from Object Video.
8. The video encoder shall have provisions for a micro-SD card for each channel input. The video encoder shall be capable of recording JPEGs for alarm conditions on customer-supplied SD cards.
9. The video encoder shall support daisy chaining up to 4 encoders together to minimize the number of network ports utilized on a switch.
10. The video encoder shall provide for 1 line level audio input per video input.
11. The video encoder shall provide for 1 alarm input per camera input. The encoders shall also provide a single relay output per unit.
12. The video encoder shall support PTZ cameras by way of Coaxitron or Pelco D protocol through a serial connection to the RS422 port.
13. The video encoder shall be capable of digitally signing each frame of video to guarantee the authenticity of digital video all the way back to its source.
14. The video encoder shall support SNMP diagnostic messages and traps and shall be compliant with SNMP versions 1 and 2.
15. The video encoder shall use a standard web browser interface for remote administration and configuration of encoder and camera settings. The browser interface shall support multi-screen remote monitoring for cameras attached to other encoders or cameras with Sarix technology on the same network subnet.
16. The video encoder shall meet or exceed the following design and performance specifications:

a. Power Consumption

1) 1-Channel Models

a) 12 VDC or 24 VAC	15 W (52 BTU/h)
b) 802.3af PoE	12 W (41 BTU/h)

c) 12 VDC (rack)	75 W (256 BTU/h)
2) 2-Channel Models	
a) 12 VDC or 24 VAC	17.5 W (60 BTU/h)
b) 802.3at PoE+	14 W (48 BTU/h)
c) 12 VDC (rack)	75 W (256 BTU/h)
3) 4-Channel Models	
a) 12 or 24 VDC	27.5 W (94 BTU/h)
b) 12 VDC (rack)	70 W (239 BTU/h)
c) Power Input	
i. 12 VDC	±10%
ii. 24 VAC	±10%
d) Power Connectors	
i. 1 and 2 channel	4 pin connection or PoE
ii. 4 channel	4 pin connection
b. Environmental Specifications	
1) Operating Temperature	
a) 1- and 2-Channel	32° to 113°F (0° to 45°C)
2) 4-Channel Models	41° to 95°F (5° to 35°C)
a) Operating Humidity	20% to 80%, noncondensing
b) Max. Humidity Gradient	10% per hour
c) Operating Altitude	–50 to 10,000 ft (–16 to 3,048m)
d) Operating Vibration	0.25 G at 3 Hz to 200 Hz at a sweep rate of 0.5 octave/minute
c. Physical Specifications	
1) Construction	Sheet metal
2) Finish	Gray metallic, black matte finish
3) Dimension	10.43” D x 6.55” W x 1.08” H (26.5 x 16.4 x 2.7 cm)
4) Mounting	Desktop (feet), or wall as per Contract Drawings
5) Unit Weight	2.0 lbs. (0.9 kg)
d. System Specifications	
1) Video Standards	NTSC
2) Video Coding	MJPEG and H.264 Baseline, Main and High
3) Video Streams	3 independently configurable per video channel