SECTION 28 00 10
SECURITY GENERAL

PART 1: GENERAL

1.01 DESCRIPTION:

A. These Security Systems General provisions apply to the following:

1. Section 28 10 00, Security Systems.

2. Section 28 11 00, Video Surveillance Systems.

B. Security systems Performance Verification is specified in Section 28 00 90, Security Performance Verification.

C. The interfacing power of and grounding provisions with work provided under these Sections is covered under these Sections.

1.02 DEFINITIONS

A. Words that are in common use are used throughout the Drawings and Specifications, except:

1. Words which have well-known technical or trade meanings are used in accordance with such recognized meanings.

2. Whenever the following listed words and phrases are used, they shall be mutually understood to have the following respective meanings:

B. The words "as indicated." means: as shown on the Drawings, and in accordance with the Specifications.

C. The words "as required." means: as required to provide a complete and satisfactory Work in full conformance with the Drawings and Specifications.

D. The word "New" means: new Work to be provided by Contractor.

E. The word "Provide" means: furnish, install, connect, test and make ready for use.

F. The words "Relocate existing" means: remove existing item from present location. Reinstall, re-connect, and test existing item and make ready for use at new location as shown on the Drawings.

G. The words "Remove existing“ means: remove existing item and return item to the Owner.

H. The word "Replace" means: remove existing item and return item to the Owner. Provide new item as indicated.

I. The word "Work": The Work is the completed construction required by the Drawings and Specifications, and includes all labor necessary to produce such construction, and all materials and equipment incorporated or to be incorporated in such construction.

J. The word "Furnish" means: supply item as specified. Item to be installed by others.

K. Infrastructure: As used herein shall mean conduit, raceway with all required boxes, fittings, connectors and accessories; completely installed..

1.03 QUALITY ASSURANCE:

A. Provision of manufactured components, installation, wiring and testing shall be the responsibility of a single Contractor.

B. Qualifications of Contractor:

1. Contractor shall be an installation and service contractor regularly engaged in the sale, installation, maintenance and service of access control systems.

2. Contractor shall have ten years experience with the installation, start-up and programming of systems of a similar size and complexity to the one proposed.

3. Contractor shall be a factory authorized dealer of the system proposed for at least two years.

C. Supervision Of Work:

1. Contractor shall employ a competent Foreman to be in responsible charge of the Work. Foreman shall be on the project site daily during the execution of the Work.

2. Contractor's Foreman shall be a regular employee, principal, or officer of Contractor, who is thoroughly experienced in projects of a similar size and type. Contractor shall not use contract employees or Subcontractors as Foremen.

D. Qualifications Of Technicians:

1. All security systems Work shall be performed by electronic technicians thoroughly trained in the installation and service of specialty low-voltage electronic systems.

2. Journeyman Wireman electrical workers may be used to install conduit, raceways, wiring, and the like, provided that final termination, hook-up, programming, and testing is performed by a qualified electronic technician, and that all such Work is supervised by the Contractor's Foreman.

3. All incidental Work, such as cutting and patching, lock hardware installation, painting, carpentry, and the like, shall be accomplished by skilled craftspersons regularly engaged in such type of work. All such Work shall comply with the highest standards applicable to that respective industry or craft.

4. All 120 VAC power wiring and connections are to be performed by a qualified Journeyman Wireman, licensed to perform such Work in the State of West Virginia.

E. Subcontractors:

1. Definition: A Subcontractor is a person or entity who has a direct contract with the Contractor to perform any of the Work at the site.

2. Use of any Subcontractor is subject to the approval of the Owner. The Contractor shall identify all Subcontractors on the Bid Form. The Contractor shall make no substitution for any Subcontractor previously selected without approval from the Owner.

3. Contractor's Foreman shall be on the project site daily during all periods when Subcontractors are performing any of the Work. Contractor's Foreman shall be in responsible charge of all Work, including any Work being performed by Subcontractors.

4. By an appropriate written agreement, the Contractor shall require each Subcontractor, to the extent of the Work to be performed by the Subcontractor, to be bound to the Contractor by the terms of the Drawings and Specifications, and to assume toward the Contractor all the obligations and responsibilities which the Contractor, by these documents, assumes toward the Owner.

F. Regulatory Requirements:

1. All Work is to conform to all building, fire, and electrical codes and ordinances applicable in the State of West Virginia. In case of conflict between the Drawings/Specifications and codes, the codes shall govern. Notify the Owner's Project Manager of any such conflicts.

2. Contractor shall secure and pay for all licenses, permits, plan reviews, engineering certifications, and inspections required by regulatory agencies. Contractor shall prepare, at Contractor's expense, any documents, including drawings that may be required by regulatory agencies.

3. Specifications, standards and codes: all work shall be in accordance with the following:

   a. The 2008 edition of the National Electrical Code (NFPA 70).

   b. Telecommunications Industries Association (TIA)

   c. Electronic Industries Association (EIA)

   d. Underwriters Laboratories (UL)

   e. Occupational Safety and Health Administration (OSHA)

   f. Local city and county ordinances governing electrical work.

   g. In the event of conflicts, the more stringent provisions shall apply.

G. Permits:

1. The Contractor shall apply for and obtain any and all permits required by federal, state, county, city, or other authority having jurisdiction over the work.

H. Supply only new equipment, parts and material currently manufactured at the time of submittal, and operate only for testing as part of installation procedure.

I. Conduit sizes specified herein or indicated on the Drawings refer to the standard trade sizes, are for identification purposes only, and are not actual dimensions.

J. Codes, standards and regulations referred to are minimum standards. Where the requirements of these specifications or drawings exceed those of the codes, standards and regulations, the drawings or specifications govern.

K. The drawings and specifications are complementary to each other and what is called for by one shall be as binding as if called for by both. If a discrepancy exists between the Drawing and Specifications, the higher cost shall be included, and the engineer shall be notified of the discrepancy.

1.04 DRAWINGS:

A. Drawings are generally diagrammatic and show the arrangement and location of pathways, outlets, support structures and equipment. The Contractor shall carefully investigate the structural and finish conditions affecting his work and arrange his work accordingly. Should conditions on the job make it necessary to make adjustments to pathways or materials, the Contractor shall so advise the Engineer and secure approval before proceeding with such work.

B. Where exact locations are required by equipment for stubbing-up and terminating conduit concealed in floor slabs, the Contractor shall request drawings, equipment location drawings, foundation drawings, and any other data required by him to locate the concealed conduit before the floor slab is poured.

C. Materials, equipment, or labor not indicated but which can be reasonably inferred to be necessary for a complete installation shall be provided. Drawings and Specifications do not undertake to indicate every item of material, equipment or labor required to produce a complete and properly operating installation.

D. The right is reserved to make reasonable changes in locations of equipment indicated on Drawings prior to rough-in without increase in contract cost.

E. The Contractor shall not reduce the size or number of conduit runs indicated on the Drawings without the written approval of the Engineer.

F. Any work installed contrary to Contract Drawings shall be subject to change as directed by the Engineer, and no extra compensation will be allowed for making these changes.

G. The location of equipment, support structures, outlets, and similar devices shown on the Drawings are approximate only. Do not scale exact equipment locations off the Drawings. Obtain layout dimensions for equipment from Architectural plans unless specifically indicated on Electronic Security plans.

H. Schematic diagrams shown on the Drawings indicate the required functions only. The technology of a particular manufacturer may be used to accomplish the functions indicated without exact adherence to the schematic Drawings shown. Additional labor and materials required for such deviations shall be furnished at the Contractor’s expense.

I. Verify the ceiling type, ceiling suspension systems, and clearance above hung ceilings prior to ordering cabling and associated hardware. Notify the Engineer of any discrepancies.

J. Portions of these Drawings and Specifications are abbreviated and may include incomplete sentences. Omissions of words or phrases such as “the Contractor shall,” “shall be,” “as indicated on the Drawings,” “In accordance with,” “a,” “the” and “all are intended” shall be supplied by inference.

1.05 SUBMITTALS:

A. Within 15 days after notice to proceed, submit a schedule indicating the proposed submission date of each submittal specified herein. Schedule shall anticipate the submittal review time, the possible need for resubmittals, and the time required for fabrication, shipping and integration into the construction sequence. Engineer will advise of any conflicts in reviewing submittals that the proposed schedule presents.

B. Submittals shall be submitted as a single package and include the following:

1. Product data:

a. Provide product data sheets for equipment, materials, and cables in PDF format. PDF submittals shall be organized in the same order as the specifications and include a table of contents and hierarchical bookmarking system to clearly identify the location of each product within the submittal. In front of each product data sheet submitted insert and complete a copy of the Cover Sheet for Submittals to Newcomb & Boyd included at the end of this Section. An electronic copy is available upon request. For each product, indicate compliance or deviation with requirements specified herein and indicated on the Drawings on the submittal cover sheet.

b. For product data sheets that contain multiple options for the same component, indicate the exact model or option provided on the submittal cover sheet and on the product data sheet by highlighting or by use of a red arrow.

c. Indicate deviations, if any, including any from the manufacturer's installation instructions.

1. Shop Drawings:

a. Reproductions or electronic versions of design drawings shall not be used in the preparation of shop drawings.

b. Floor plans and diagram shop drawings shall be prepared in AutoCAD DWG format and submitted as PDF plots on the same drawing size as the design drawings.

c. Include floor and site plans indicating equipment locations. Plans shall include equipment identification and either direct references to wiring details for each specific installation and wiring condition or a schedule that references the same.

d. Wiring diagrams shall indicate proposed connections of equipment, model numbers, and designations for cables and termination points.

e. Provide elevations of console or rack-mounted equipment, showing the location of all specified electronics and include enlarged, to scale plan (top), and front views.

f. The specification of sizes and dimensions shown in the drawings shall have a tolerance of not more than +/- 0.05".

g. Provide project specific manufacturer shop drawings of fabricated or modified units, if any.

h. Provide UPS load calculations.

i. Provide riser diagrams indicating components of the system and proposed cabling between these components.

j. Provide block diagrams indicating the proposed interface between the access control system, intercom system, video surveillance system, and fire alarm system. Provide a written description of the proposed sequence of operation to describe the operation of the interfaces.

k. Provide typical wiring diagrams indicating the interface between door hardware provided under Division 8 for each door type and a written description of the door's sequence of operation. Reference door hardware interface wiring diagrams for each door on the floor plans or on a door schedule.

l. Provide detailed project specific mounting diagram for each type of device including raceway and backbox requirements. These details shall be referenced on the floor plans or schedules.

m. Provide proposed elevation for each security enclosure location, including equipment identification and model/part numbers.

n. Provide a detailed loading schedule for each security control panel, video surveillance switch, patch panel, network video server recorder, or other head-end equipment identifying each device connected to it.

o. Provide proposed project specific raceway layouts including conduit sizes, and backbox sizes.

p. Provide detailed full-scale drawings of each alarm screen with icons. Provide a schedule of icons that includes a written description for the functionality of each icon.

C. Submittals not specifically required, or not complying with the format requirements, will be returned un-reviewed.

D. Submittals are required before installation begins. Equipment shall not be ordered, and pay requests will not be approved prior to receipt and approval of submittals.

1.06 ENVIRONMENTAL REQUIREMENTS:

A. Systems or equipment installed in environmentally controlled areas shall meet performance requirements specified herein in the following conditions:

1. Temperature: 40°F to 95°F.

2. Humidity: 20% to 80% RH.

3. Air purity: systems shall be capable of continuous operation in an environment where the level of dust, lint, paper fiber, and other airborne particles is equal to that found in a standard office.

B. Systems or equipment installed in indoor environmentally uncontrolled areas shall meet performance requirements specified herein in the following conditions:

1. Temperature: 0°F to 120°F.

2. Humidity: 5% to 95% RH.

C. Systems or equipment installed in outdoor areas shall meet performance requirements specified herein in the following conditions:

1. Wind-driven dust, dirt, sand, and snow for 6 hours.

2. Rain at a maximum rate of 4" per hour.

3. Ice loads up to 2" measured radially to exposed surfaces.

4. Wind: 85 mph, maximum.

5. Sleet with wind: 55 mph, maximum.

6. Snow cover: 2' maximum, measured vertically.

7. Humidity: 0% to 100% RH.

8. Temperature: -30°F to 150°F.

1.07 SPACE CONDITIONS:

A. Verify dimensions of equipment, equipment arrangements, space availability (including any millwork or cabinetry provided by others) and provide systems that work within the constraints of the space available. Notify the Engineer of any situation where space constraints are a problem, prior to the ordering or purchase of equipment. The Contractor shall bear the expense of providing alternate equipment, which will work within the available space, if space availability problems are discovered after equipment is ordered.

B. Drawings are diagrammatic in nature and, unless explicitly dimensioned, indicate approximate locations of equipment and components. Changes in the location, and offsets, of same which are not shown on the Drawings but are necessary in order to accommodate building conditions and coordination with the work of other trades, shall be made prior to initial installation, without additional cost to the Owner.

C. Provide access to equipment and components requiring operation, service or maintenance within the life of the system.

1.08 WARRANTY:

A. Equipment shall be free of faulty workmanship and defects for a period of 1 year from date of substantial completion.

B. Replace defective materials and repair faulty workmanship within 2 days of notification at no cost to the Owner during warranty period.

C. In addition to warranty, provide maintenance service for the warranty period, including at least 2 semi-annual visits to site for checking and adjustment of equipment. During this period, answer service calls within 24 hours. During this period, maintenance calls shall be completed within 3 days of notification and at no cost to the Owner.

D. Software/firmware maintenance: new releases or updates of hardware, software, applicable user manuals, technical and alert bulletins released by the access control manufacturer shall be applied to the system at no cost to the Owner during the warranty period.

PART 2: PRODUCTS

2.01 Interior Floor-Mounted Equipment Cabinets:

A. Minimum 16 gauge steel construction.

B. Enclosed with ventilated side panels, square front and vertical corners.

C. Minimum 18" deep.

D. Configured for standard 19" rack panels.

E. Coordinate height as indicated on the Drawings. with the equipment used.

F. Finish color shall be black.

G. Manufacturer: Amco, Atlas/Soundolier, Hammond, HOME, Lowell, Middle Atlantic Products, Stantron, or Winsted.

2.02 NETWORK EQUIPMENT:

A. Patch Panels:

1. Patch panels shall be rated to meet Category 6 channel warranty requirements.

2. Integrated labels for front and rear.

3. Maximum ports: 48.

4. Rear cable manager.

5. Panels shall be modular type and shall allow standard jacks to be utilized.

6. Manufacturer: Panduit or approved equal.

B. Data Patch Cords:

1. Factory-assembled plug ended jumpers for patch panel blocks.

2. Modular data patch cords shall meet Category 6 channel performance requirements specified herein, and shall be #24 AWG tinned-copper, stranded conductors insulated with solid polyolefin, tightly twisted into individual pairs and jacketed with flame-retardant PVC.

3. Manufacturer: Panduit or approved equal.

2.03 AC POWER:

A. General:

1. Except as otherwise specified herein or indicated on the Drawings, grounding conductors shall be insulated. Insulation shall be rated 600 V. Conductors shall be continuous from connector to connector with no splices. Grounding connectors shall be solid bronze, compression type, designed for use intended.

2. Power wiring for the extension of power circuits provided by others shall be #12 AWG THWN/THHN or XHHN, 600 V, rated at 194°F.

3. AC power equipment shall have LED or lamp status devices to provide indication that the systems are on.

B. Surge protection devices (SPDs): SPDs shall incorporate silicon avalanche technology, shall operate bi-directionally, and have a turn-on and turn-off time of less than 5 nanoseconds. Additional minimum requirements include:

1. Communication or Signal Conductor Transient Suppressors:

a. Non-coaxial SPDs shall be UL listed in accordance with UL 497B-2011.

b. Maximum single impulse current conductor-to-conductor or conductor-to-ground: 10000 A, 8 x 20 µs waveform, or 200 A, 10 x 1000 µs waveform.

c. Pulse life rating: 3000 A, 8 x 20 µs waveform, 2000 occurrences, or 50 A, 10 x 1000 µs waveform, 200 occurrences.

d. Maximum clamping voltage at 100 A, 10 x 1000 µs waveform, with the peak current not to exceed the normal applied voltage by 150%, except for coaxial cable suppressors with peak current, the maximum clamping voltage shall not exceed the normal applied voltage by 200%.

e. Failure mode: fail short.

2. AC Voltage Power Transient Suppressors:

a. Outlets shall have integral transient suppression in accordance with IEEE C62.41.1-2002 (R2008), IEEE C62.41.2-2002, IEEE C62.45-2002 (R2008), and UL 1449-2006.

b. Maximum single impulse current rating: 75000 A, 8 x 20 µs waveform.

c. Pulse life rating: 30 occurrences at 15000 A, 8 x 20 µs waveform, and 150 occurrences at 10000 A, 8 x 20 µs waveform.

d. Maximum clamping voltage shall not exceed 350 V peak for a 120 V nominal voltage source at 3000 A, 8 x 20 µs waveform.

e. Visible indication of proper suppressor connection and operation.

3. Manufacturer: Advanced Protection Technologies, Emerson, Lightning Eliminators & Consultants, or Transtector.

C. Ground Bus Bars:

1. Solid copper, minimum 6" x 0.75" x 0.25".

2. Free from surface corrosion.

3. Drilled and tapped 0.25-20 and 10-24 to terminate incoming conductors individually.

2.04 UNINTERRUPTIBLE POWER SUPPLY (UPS):

A. Desktop UPS:

1. Line interactive topology. Capacity as required for the equipment powered.

2. System shall be a self-contained unit designed for the support of computers.

3. Batteries: lead-calcium, lead-acid, or nickel-cadmium type sized to sustain the UPS at full rated load for 10 minutes, and half rated load for 30 minutes.

4. Integral lightning and surge protection complying with IEEE C62.41.1-2002 (R2008), IEEE C62.41.2-2002, and UL 1449-2007.

5. The UPS shall provide the following characteristics:

   a. Nominal input voltage: 120 VAC.

   b. Integral automatic current and overvoltage protection.

   c. Electrical noise isolation: 5 dB to 45 dB common mode, 28 dB to 80 dB normal mode.

   d. Recharge time: less than 10 hours.

   e. Transfer time: 0 ms.

   f. Efficiency: 95%.

6. Manufacturer: APC, Eaton, or Tripp-Lite.

B. Rack-Mounted UPS:

1. Line interactive topology. 2200 VA (1920 W) capacity.

2. System shall be a self-contained rack mountable unit designed for the support of computers.

3. Audible noise shall not exceed 52 dBA at 3' .

4. Batteries: lead-calcium, lead-acid, or nickel-cadmium type sized to sustain the UPS at full rated load for 30 minutes, and half rated load for 60 minutes.

5. Integral lightning and surge protection complying with IEEE C62.41.1-2002 (R2008), IEEE C62.41.2-2002, and UL 1449-2007.

6. The UPS shall provide the following characteristics:

   a. Nominal input voltage: 120 208 220 240 V AC.

   b. Integral automatic current and overvoltage protection.

c. Electrical noise isolation: 5 dB to 45 dB common mode, 28 dB to 80 dB normal mode.

d. Recharge time: less than 10 hours.

e. Transfer time: 0 ms.

f. Efficiency: 95%.

7. Manufacturer: APC, Eaton, or Tripp-Lite.

2.05 SLEEVES:

A. Wall sleeves shall be galvanized rigid metal conduit or electrical metallic tubing.

B. For floor slabs above grade, plastic core form block-outs shall be used.

2.06 PENETRATION SEALS:

A. Firestops:

1. Firestops shall consist of an asbestos-free fill material, forming/backing/damming materials, and accessories needed to complete a UL classified through-penetration firestopping system. Fill material shall not slump or sag and shall be the required thickness in the fully cured state.

2. Firestops shall be designed to seal through-penetrations against flame, heat, smoke, and water in compliance with ASTM E84-2013a, ASTM E119-2012a, ASTM E814-2013, and UL 723-2008.

3. Firestops shall be specifically designed and rated for the individual application, including movement, materials, moisture, penetrating item material, and fire and smoke ratings of the penetrated construction.

4. Manufacturer: 3M, GE, Flammadur, Hilti, Nelson, Rectorseal, or Thomas & Betts.

B. Expansion Seals:

1. Waterproof, modular, mechanical expansion type consisting of synthetic rubber grommets or interlocking links shaped to continuously fill the annular space between the penetrating item and the opening. Sizing of links and sleeve shall be determined by the manufacturer.

2. Manufacturer: Calpico Pipe Linx, Metraflex MetraSeal, or Thunderline Link Seal.

C. Seal Assemblies:

1. Seal assemblies shall consist of a frame, compression mechanism, and insert modules. Assemblies shall be waterproof and shall be designed to allow easy addition or deletion of penetrating items.

2. Seal assemblies for multicable penetrations of fire- and smoke-rated construction shall comply with the requirements of firestops as specified herein.

3. Manufacturer: Nelson Multi-Plug.

2.07 CABLES, CONNECTORS AND MISCELLANEOUS EQUIPMENT:

A. General:

1. Cable construction, insulation, and jacket shall comply with NFPA 70-2008, requirements for the application for which it is used. Provide type CM or CMG for general use; type CMP for plenum use; and CMR for riser use.

2. Cables and conductors installed in enclosures or raceways underground or in slabs on grade shall be UL listed for use in wet locations.

3. Flame resistance: non-plenum rated cable shall comply with UL 1581-2001. Plenum-rated cable shall comply with NFPA 262-2011.

B. Alarm Cabling:

1. Two unshielded twisted pair, #22 AWG or larger cable (sized for voltage drop) for cabling between addressable alarm or sensor devices.

2. Unshielded 4-conductor, #20 AWG or larger cable (sized for voltage drop) for cabling to motion detection devices.

3. Unshielded 2-conductor, #20 AWG or larger cable (sized for voltage drop) for cabling to door contacts.

4. Manufacturer: Alpha, Belden, CommScope, or West Penn.

C. RS-232 Cable:

1. Two twisted pairs, #22 AWG, stranded (7x30) tinned copper conductors, each pair individually shielded with aluminum foil-polyester tape to provide 100 percent shield coverage.

2. Pairs shall be cabled on common axis with #24 AWG, stranded (7x32) tinned copper drain wire.

D. RS-485 Cable:

1. Two unshielded twisted pairs, #22 AWG, stranded (7x30) tinned copper conductors.

E. Control Cables:

1. Multiconductor, color-coded type, #22 AWG or larger conductors (sized for voltage drop), stranded tinned-copper for energy limited control circuits. Multiconductor, color-coded type, #14 AWG or larger conductors (sized for voltage drop), stranded tinned-copper for other control circuits.

F. Network Cables:

1. UL listed and CSA certified.

2. Category 6 cables meeting TIA/EIA 568-B1-B3, with addenda, requirements for category 6 cable.

3. Additional Cable Performance Requirements:

a. Minimum power sum ACR: 9 dB at 155 MHz.

b. Maximum attenuation: 21 dB at 100 MHz per 100 m.

c. Minimum power sum near end crosstalk: 36 dB at 100 MHz.

d. Minimum power sum near end crosstalk: 36.3 dB at 250 MHz.

e. Minimum power sum equal level far end crosstalk: 16.8 dB at 250 MHz.

f. Maximum delay skew: 25 ns.

2.08 IDENTIFICATION MATERIALS:

A. Nameplates: white core plastic laminate with engraved lettering.

B. Nameplates for individual devices shall have 0.25” high letters.

2.09 RACEWAYS AND BOXES:

A. Raceways:

1. Raceway components shall be new and UL listed.

2. Electrical metallic tubing shall be galvanized steel. Connectors and couplings shall be malleable iron or steel, galvanized or cadmium-plated, compression or set screw type. Connectors shall have insulated throats.

3. Flexible metal conduit shall be galvanized steel. Connectors shall be of the twist-in, insertion or totally enclosed clamp type, galvanized malleable iron or steel, with insulated throats.

4. Liquidtight flexible metal conduit shall be extra flexible type, neoprene-jacketed. Connectors shall be watertight, of the twist-in, insertion type, galvanized malleable iron or steel, with insulated throats.

5. Rigid metal conduit shall be galvanized steel. Connectors and couplings shall be threaded galvanized malleable iron or steel. Locknuts shall be of the type with sharp edges that bite into enclosure where connected. Plastic insulating bushings shall be high temperature type. Sealing bushings shall have galvanized malleable iron locking ring with molded neoprene sealing ring with predrilled holes to accommodate each individual conductor, stainless steel screws and washers, PVC-coated pressure discs, and factory-installed lay-in grounding conductor lugs. Hub fittings shall be 2-piece, insulated throat, liquidtight type of steel or malleable construction.

6. Rigid nonmetallic conduit shall be rigid polyvinyl chloride, non-burning, high impact, schedule 40 or type DB. Couplings and connectors shall be rigid polyvinyl chloride, high impact, schedule 40. Cement for connections of conduit shall be approved by the conduit manufacturer.

7. Surface-mounted raceway shall be two-piece, surface metal type for power and communications service, consisting of base and cover sections. Raceways shall be capable of being internally divided into 2 separate equal compartments for power and communications wiring. Raceway system shall be complete with fittings, elbows, couplings, wire retainer clips, blank ends, and transition pieces to other surface metal raceways and to 0.5" to 1.5" conduit. Raceway system shall also be complete with device brackets for horizontal or vertical single- or double-gang devices, and combination receptacle and telephone outlet covers.

B. J-Hooks:

1. J-hooks shall be steel, UL listed for a maximum static load of 50 lbs, and shall be rated for use in plenum environments.

C. Boxes:

1. Boxes shall be the type, size and configuration required for its specific use, location, device, and number, size, and arrangement of raceways connecting thereto.

2. Outlet boxes shall be constructed of code-gauge galvanized steel, unless otherwise specified herein. Where installed in hazardous locations or exposed to corrosive atmosphere, rain or spray, boxes shall be corrosion-resistant cast metal with threaded entrances, removable covers, gaskets, and corrosion-resistant screws.

a. Outlet boxes recessed in plaster or gypsum board walls or columns shall be 4" or 4.688" square, 2.125" deep with plaster rings.

b. Outlet boxes surface-mounted on walls or columns shall be 4" square, 2.125" deep, with no plaster ring or knock-outs.

c. Outlet boxes for devices recessed in metal door jambs shall be sheet metal partition boxes sized for the application.

d. Outlet boxes recessed in masonry walls shall be square cornered masonry boxes or standard 4" square boxes fitted with square cornered tile covers of proper depth for block. Both type boxes shall be 2.125" minimum depth.

e. Outlet boxes recessed in ceilings shall be 4" octagonal or square, 2.125" depth.

f. Outlet boxes recessed in concrete shall be UL approved for the application.

g. Through-wall type outlet boxes are not acceptable.

h. Where special purpose devices require a larger outlet box than specified herein, provide outlet boxes for each specific device.

i. Boxes containing low voltage and line voltage devices shall have metal barriers.

j. Manufacturer: Appleton, Crouse-Hinds, Efcor, Midland Ross, O-Z/Gedney, Raco, or Steel City.

PART 3: EXECUTION

3.01 GENERAL:

A. Install plenum rated cables where cables are not installed in conduits or enclosed wireways.

B. Cables and conductors installed in enclosures or raceways underground or in slabs on grade shall be UL listed for use in wet locations.

C. Provide incidental equipment or devices to provide a complete and operable system.

D. Verify equipment model numbers and conformance of each component with manufacturer's specifications.

E. Equipment shall be installed in accordance with the manufacturer's instructions.

F. Equipment, except portable equipment, shall be held in place. This shall include equipment, enclosures, components, and cables. Fastenings and supports shall support their loads with a safety factor of at least 3 unless otherwise specified herein.

G. Prevent and guard against electromagnetic and electrostatic hum, and install the equipment to provide safety for the operator.

H. Repair or replace any equipment or materials damaged during the construction period.

I. Provide power connections to specialty equipment and as indicated on the Drawings.

J. Exposed equipment, equipment supports, and components in the telecom rooms shall have a flat dark gray finish unless otherwise specified herein.

K. Patch, paint, and otherwise restore to original condition walls, floors, and ceilings cut, modified, or damaged in the process of implementing this Work.

3.02 EQUIPMENT ENCLOSURES:

A. Where controls or equipment are specified herein or indicated on the Drawings for future installation, space shall be provided in the control console and the equipment racks, and on the control panels.

B. Provide ventilation according to equipment manufacturer's recommendations.

C. Provide unused equipment enclosure panel space with blank or ventilating panels.

3.03 NETWORKED EQUIPMENT:

A. Configure the network addresses, security settings, and other parameters per the Owner's requirements and as recommended by the manufacturer to support the security systems and video surveillance systems as indicated on the Drawings.

3.04 SLEEVES:

A. Provide where conduits pass through elevated floor slabs if conduits are not a part of the slab pour and for future cable or conduit risers.

1. Install in raised foundations at least 2" high.

B. Provide where cables pass through walls and elevated floor slabs.

C. Wall sleeves shall extend 4" from each side of the walls.

D. Openings through slabs for busway risers shall be finished with a 4" wide x 2" high curb around the opening.

E. Sleeves shall be secured in place. Provide insulating bushings on both sides of sleeves for cables.

F. Provide ground bushings on both sides of sleeves containing separate ground conductors.

3.05 PENETRATION SEALS:

A. General:

1. Install in accordance with the manufacturer's published instructions to achieve ratings and classifications specified herein. A copy of these instructions shall be maintained and available on site.

B. Firestops:

1. Close and firestop abandoned penetrations and penetrations through fire- and smoke-rated construction. Materials used to seal these penetrations

shall continue the construction's fire and smoke resistance ratings uninterrupted and shall maintain an effective barrier against the spread of flame, smoke, water and hot gases.

2. Install after installation of raceways.

C. Expansion Seals:

1. Install to seal single conduit or cable penetrations of walls below grade.

D. Seal Assemblies:

1. Install to seal the penetration of walls below grade by multiple cables in the same opening.

3.06 CABLES, CONNECTORS AND MISCELLANEOUS EQUIPMENT:

A. General:

1. Make joints and connections with 60/40 resin-core solder or mechanical connectors. Temperature-controlled soldering irons rated at least 60 W shall be used for soldering work.

2. Inter-rack cabling shall be strapped, dressed, and supported. Intra-rack wiring shall be completed in the shop.

3. Terminal blocks, boards, strips, and connectors shall be provided for cables, which interface with racks, cabinets, consoles, enclosures, and equipment modules.

4. As a general practice, power cables, and high level signal cables shall be run on the left side of an equipment rack as viewed from the rear. Other cables shall be run on the right side of an equipment rack, as viewed from the rear.

5. No cable shall be installed with a bend radius less than that recommended by the cable manufacturer.

6. Unused cables shall be dressed at each end in heat-shrink tubing and marked as unused.

7. Heat-shrink tubing shall be used to insulate and dress the ends of outdoor wires and cables, including a separate tube for the ground or drain wire.

8. No cables shall be wired with a polarity reversal between connectors, at either end. Special care shall be taken when wiring to ensure that constant polarity is maintained.

B. Network Cable:

1. Security network cables shall be installed in a star topology from each security network patch panel to the security equipment being served on the same floor. The length of this cable shall not exceed 295'. Coordinate the cable routing as necessary to ensure distance requirements are not exceeded.

2. Observe the bending radius and pulling strength requirements of the cables during handling and installation. Each run of cable between the patch panel and the network outlet serving the security equipment shall be continuous without joints or splices.

3. Conceal security network cables within ceilings and walls. Complete work above ceiling prior to ceiling tile installation.

4. Cables shall be routed at least 2' from any fluorescent ballast and at least 40" from any electric motors or other high level source of EMI.

5. Cabling routed above ceilings shall be supported using the following methods:

a. In cable tray above accessible ceiling where indicated on the Drawings.

b. In conduit where indicated on the Drawings.

c. On J-hooks, unless otherwise indicated on the Drawings.

6. Cables, when not installed in conduit or cable tray, shall be bundled in groups of 25 and cable tied. Cable ties shall not be tight to the point of deforming the cable jackets.

7. Provide temporary protection of cables before termination. Cables shall not be left lying on the floor. Bundle and use cable ties to provide protection.

8. Provide clutch or shear pin protection for cables during cable pulling to ensure cable pulling tension is not exceeded.

9. Jacks shall be wired per the pair assignments indicated in the TIA/EIA 568-B1-B3, with addenda, designation T568B wiring plan.

10. Network cables shall be installed and terminated in accordance with the manufacturer's recommended procedures.

C. Network cross-connects:

1. Copper data cross-connects shall consist of 19" rack mounted patch panels. If more than 48 cables are to be terminated in a single rack, a patch cord organizer shall be placed between 48-port cross-connect units.

2. If only one cross-connect panel is required a patch cord organizer shall be placed under the panel. Horizontal cables shall be terminated directly onto this modular panel.

3. Provide 2 patch cords for each camera data jack. 50% shall be nominal 7':, 50% shall be nominal 3' in length.

D. Receptacles and Connectors:

1. Unless otherwise specified herein, female type receptacles shall be used for floor, wall and panel mountings. Male type connectors shall be used for cable mountings.

2. Provide strain relief on connectors.

3. Provide faceplates for receptacles as indicated on the Drawings.

4. Receptacles shall be insulated from the mounting panel, outlet box, or wireway. Unless otherwise specified herein, this shall be accomplished by using insulated-from-panel type receptacles.

5. Provide blank coverplates for boxes intended for future use, unless otherwise indicated on the Drawings.

6. Insulate cables from receptacle faceplates.

E. Surge Protection Devices:

1. Install on low voltage signal or communications conductors entering the building from exterior locations, including those conductors from devices mounted on the exterior of the building.

2. Provide AC power SPDs on microprocessor-based specialty system rack-mounted equipment.

3.07 IDENTIFICATION:

A. General:

1. Identification shall consist of upper case letters.

2. Where identification is applied to surfaces which require a finish, identification shall be installed after the surface has been finished.

B. Cables:

1. Cables, regardless of length, shall be marked with preprinted, wrap-around number or letter cable markers at both ends. Markers shall be permanently affixed with heat-shrink tubing. There shall be no unmarked cables at any place in the system. Marking codes used on cables shall be indicated on the record drawings.

C. Equipment:

1. Provide and install engraved labels for each item rack-mounted equipment.

2. Except where otherwise specified herein, label switches, controls, and receptacles. Labeling material shall be engraved plastic laminate or metal plates. Labels shall be placed on coverplates or directly adjacent to switches, controls, and receptacles to facilitate service and replacement.

3. Signs shall not cause interference with operation and maintenance of equipment. Attach signs with rustproof screws.

3.08 RACEWAYS AND BOXES:

A. Raceways:

1. Unless otherwise indicated on the Drawings or specified herein, minimum raceway size shall be 0.75". Install the raceway systems in compliance with manufacturer's written instructions.

2. Where raceways must pass through structural members, obtain approval from the Engineer regarding location and size of openings prior to drilling. Lateral raceways in masonry shall not exceed 0.75".

3. Raceways that pass through expansion joints shall be provided with expansion fittings. Raceways shall be run parallel with or at right angles to the building walls.

4. Raceways shall be secured in place and protected to prevent damage to the work during construction. Open ends of raceways shall be taped or capped after installation to prevent entry of dirt and debris during construction prior to pulling wire. Installation of raceways shall be complete and shall be blown-out and swabbed clear of water and trash prior to pulling wire.

5. Install junction or pull boxes to avoid excessive runs or bends. Provide pull lines in empty raceways. At each end, leave 12" of slack coiled in the box, or at the end of the conduit where boxes are not installed, and secure at each end.

6. Electrical metallic tubing shall be installed for specialty systems conduits, except underground or below slab on grade. Electrical metallic tubing stubbed-up from floor slabs or down from ceiling plenums and not connected to an enclosure shall terminate with an insulated throat connector.

7. Flexible metal conduit shall be installed for connections to electrical equipment subject to movement or vibration.

8. Liquidtight flexible metal conduit shall be installed for connections to electrical equipment subject to movement or vibration where exposed to rain, spray, or a corrosive atmosphere.

9. Rigid metal conduit shall be installed for applications not otherwise specified herein. Rigid metal conduit shall be secured to metal enclosures using hub fittings. Insulated bushings or fittings shall be installed at connections to cabinets and boxes. Terminate stub-ups not attached to enclosures with an insulated throat grounding bushing. Commercial pipe joint compound shall be applied to the male threads on threaded joints and fittings. Connections shall be wrenchtight, and where subject to ground water, rain or spray shall be watertight.

10. Rigid nonmetallic conduit may be used in lieu of rigid metal conduit, or electrical metallic tubing, where permitted by local codes, unless otherwise specified herein. Install with conduit supports spaced not further apart than:

Size	Spacing
1" and less nominal conduit	2'-6"

1.25" to 2" nominal conduit	5'
2.5" and larger nominal conduit	6'

Do not install in air ducts or return air plenums. An insulated copper grounding conductor shall be installed in each plastic conduit unless prohibited by local codes or utility company. Grounding conductors shall be bonded to grounded metal enclosures or devices at origin and at each outlet. Rigid nonmetallic conduit shall not be used for attachment to boxes of outlets stubbed-up above the finished floor. A transition to rigid metal conduit shall be made a minimum of 18" from each outlet.

11. Install electrical nonmetallic tubing or intermediate metallic tubing for conduits embedded in poured concrete construction above grade.

B. Boxes:

1. Install boxes at each device, and outlet, and where indicated on the Drawings. Coordinate box installation with conductor/cable and raceway installation. Coordinate box installation with other trades so that boxes will remain accessible. Outlet boxes shall not be installed back-to-back. Maintain minimum 24" separation between outlet boxes on opposite sides of rated walls, and minimum 6" separation in nonrated walls. Install boxes level, plumb, and square to the structure. Anchor boxes in place. Provide knockout closures to cap unused knockout holes where blanks have been removed.

2. The approximate locations of outlets are indicated on the Drawings. The exact locations shall be determined at the building. The right is reserved to change the exact location of any switch or outlet box in any room before it is permanently installed, without additional cost to the Owner and as approved by the Engineer.

3. Install outlet boxes at heights above the finished floor, measured to the centerline of the outlet, as indicated on the Drawings. Set outlet boxes for flush-mounted devices to within 0.125" of finished wall. Adjust mounting heights of boxes in masonry walls to minimize cutting and patching of masonry. Install outlet boxes in one vertical line when indicated adjacent on the Drawings but at different mounting heights. Covers on recessed ceiling outlet boxes shall be painted to match the ceiling.

4. Install exposed junction or pull boxes only in unfinished spaces, unless indicated otherwise on the Drawings.

C. J-Hooks:

1. Install maximum 5' on center.

2. Attach J-hooks to the structure as recommended by the manufacturer, except that J-hooks shall not be installed using drop wires or ceiling support wires. J-hooks shall not be connected to ceiling supports, utilities, or equipment.

3.09 EQUIPMENT AND EQUIPMENT ROOMS:

A. Remove dust, dirt, rust, stains, and temporary covers.

B. Foreign matter shall be blown, vacuumed, or cleaned out of and from new equipment, devices, switches, controls, and panels.

C. Clean and polish identification plates.

D. In equipment rooms, clean equipment, conduit, and room surfaces form dust and dirt and maintain in a clean condition form date of substantial completion until final completion of work and corrective work.

E. Remove excess material from the Project site.

3.10 GROUNDING:

A. Equipment shall be grounded as specified herein, and in accordance with the equipment supplier's recommendations.

B. A single primary specialty system ground shall be established for the specialty systems in each particular area as indicated on the Drawings and as follows:

1. In each enclosure install a copper bus bar mounted to the enclosure on insulated support blocks to act as the ground point for the connection of ground conductors used within that enclosure. Terminate insulated ground conductors to the bus bar with torqued machine screws. Bars shall be bounded to enclosures with #2 AWG insulated conductors.

2. Enclosures shall be in groups as indicated on the Drawings. Each enclosure in its group shall be grounded by installing an insulated grounding conductor from one enclosure ground bus bar to another. A single #6 AWG insulated grounding conductor from each rack group shall be run back to the insulated grounding conductor located in a dedicated junction box.

3. Conduit shall be isolated from enclosures with insulated fittings.

C. Surge Suppression Equipment Grounding:

1. Connect each suppressor to the local ground bus in the terminal cabinet with wiring sized as recommended by the manufacturer. Where M block type terminations/suppressors are used, bond the ground rail to the local ground bar with wiring as recommended by the manufacturer.

2. Coordinate to ensure that the 120 V AC power source/supply suppressor is also grounded to the same local ground bus as suppressors provided in this Section for the same system.

3.11 OPERATION AND MAINTENANCE DOCUMENTATION PACKAGE:

A. These operation and maintenance manual requirements supplement operation and maintenance manual documentation requirements of other Sections of these specifications.

B. Operation and maintenance documentation, in hardback 3-ring loose-leaf binders except full size drawings and CDs, shall cover the specialty systems. Documentation shall include operations and maintenance documentation directory, emergency information, operating manual, maintenance manual, test report, and construction documents.

C. The operating and maintenance documentation package shall be submitted as one comprehensive package to the Owner 3 weeks before systems acceptance testing, and shall be updated, revised and completed during, and at completion of, Performance Verification.

D. Documentation shall be type written and shall contain, at a minimum, the following information.

1. Introduction:

a. Project name, contractors' and subcontractors' names, addresses, and telephone and facsimile numbers.

b. Index.

2. Operations and Maintenance Documentation Directory:

a. Explanation of the identification system used, including lists of systems, equipment and component identifiers and names.

3. Emergency Information:

a. Information for technical and nontechnical personnel about actions recommended during emergency situations to protect property and to minimize disruption to the building occupants. Emergencies shall, at a minimum, include:

1) Power failure.

2) Heating failure.

3) Cooling failure.

4. Operating Manual:

a. General information for each system as applicable:

1) System features.

2) System description.

3) Simplified one-line diagrams.

4) Settings for controls.

b. Technical information for each system as applicable:

1) System specifications.

2) Operating routines and procedures.

3) User programming instructions.

4) Special procedures.

5) Basic troubleshooting.

5. Maintenance Manual:

a. Descriptions (specifications) of the equipment and components.

b. Description of function, as applicable: the function of the equipment, functional parameters, and performance verification procedures.

c. Recommended maintenance procedures and their recommended frequency for this Project.

d. Name, address and contact of at least one qualified service company.

e. Recommended list of spare parts, part numbers, and the place(s) from which they can be obtained.

f. Original purchase order number; date of purchase; name, address, and the telephone number of the vendor; and warranty information.

g. Manufacturers recommended procedures.

h. Any other information needed for the preparation of documents supporting the management of operation and maintenance programs.

i. Copies of software configuration files and/or programming files, as applicable, on CDs.

6. Test Reports and Certifications:

a. Access control and alarm monitoring system test reports.

b. Video surveillance system test reports.

c. Network cable test reports.

7. Construction Documents:

a. Record drawings.

b. Approved submittals.

c. Warranty certificates.

d. Inspection certificates.

e. Performance Verification report.

f. Tools for tamper-resistant enclosures and tools for manual resetting devices.

E. Submit a receipt signed by the Owner acknowledging receipt of the operation and maintenance documentation package.

F. Provide metal cabinets mounted on the wall of the IDF room to house the operation and maintenance documentation package. Cabinets shall be approximately 12" wide x 18" high x 6" deep constructed of 18 gauge sheet metal with hinged door with latch.

3.12 RECORD DRAWINGS:

A. Definition: Project Record Drawings are drawings that completely record and document all aspects and features of the Work. (Also known as “as-built” drawings.)

B. The purpose of Project Record Drawings is to provide factual information regarding all aspects of the Work, to enable future service, modifications, and additions to the Work.

C. Contractor shall accurately maintain Project Record Drawings throughout the course of this project. Project Record Drawings shall include documentation of all Work, including the documentation of existing equipment, wiring, conduits, and raceways that are to be reused in the Work.

D. Contractor shall maintain the working set of Project Record Drawings at the project site throughout the course of the Work. The working set shall be updated on a daily basis as the Work progresses.

E. Project Record Drawings shall accurately show the physical placement of the following:

1. Equipment and devices, including model numbers.

2. Conduit and raceways.

3. Junction and pull box locations and routing.

4. End-of-line resistor locations.

5. Interfaces to external equipment.

6. Connections to power and telephone circuits.

F. Project Record Drawings shall show the physical placement of each device and conduit or aerial center line, to be accurate to within one foot (1') of the nearest landmark. Where the site plan furnished by Owner conflicts with actual conditions, Contractor shall amend site plan as required. Indicate exact description of conduit runs (above ground, two foot trench, along outside wall of building, etc.).

G. The Record Drawings shall show wire and cable runs, zone numbers, tamper circuit configuration, panel/circuit breaker numbers from which equipment is powered, and splice points.

H. The Record Drawings shall be available for inspection by the Owner's Project Manager on a daily basis.

A. Upon completion of Work, and prior to Final Acceptance, Contractor shall prepare and submit to the Owner's representative a final record set of Record Drawings. This set shall consist of all data transferred from the working set, supplemented by Riser Diagrams and other information. The final record set of Project Record Drawings shall be drafted by a skilled draftsperson, under the supervision of Contractor. Submit the following:

1. 2 sets of bound prints.

2. 2 copies of electronic drawing files prepared in AutoCAD DWG format and PDF plot of those on CDs.

3. Two back-up copies of site-specific programs, electronic configuration files and other software to make the system operational.

B. Reproductions of design drawings shall not be used in the preparation of record drawings.

3.13 MAINTENANCE:

A. Equipment operated prior to the date of substantial completion shall be maintained in accordance with manufacturers' recommendations.

3.14 INSTRUCTION OF OPERATING PERSONNEL:

A. Conduct formal instruction sessions for operating personnel. Conduct 2 similar sessions. The first session shall be conducted at the time of start-up and check-out, and the second session shall be approximately 2 months later. Sessions shall be conducted at the site.

B. Prepare and submit a syllabus describing an overview of the program, describing how the program will be conducted, when and where meetings are to be held, names and company affiliations of lecturers, description of contents and outline for each lecture, and recommended reference material and outside reading. Obtain direction from the Owner on which operating personnel shall be instructed in each system.

C. Sessions shall include:

1. General familiarization and operating procedures for each specialty systems installation.

2. Routine maintenance procedures for equipment.

3. User level programming of programmable systems.

4. Factory-trained technicians shall give operating and maintenance instructions on the following specialty systems and equipment:

System/Equipment	MinimumSession Duration, hours
Video surveillance systems	16
Security systems	16

5. Provide DVD format video of training sessions and a complete record copy of training materials, handouts, and other printed materials used in each training session.

6. Obtain receipt acknowledging completion of each item of instruction.

END OF SECTION 28 00 10

COVER SHEET FOR
SUBMITTALS TO NEWCOMB & BOYD

Project: ______________________________ Date: ____________________

Item: ______________________________ Submittal Number: ______________

Manufacturer: ______________________________ Model: ____________________

Specification Paragraph and/or Drawing Number: ______________________________

Options Included (if any):____

____

____

____

Deviations (if any; if none, state so): ______________________________________

____

____

____

____

____

SECTION 28 00 90
SECURITY PERFORMANCE VERIFICATION

PART 1: GENERAL

1.01 DESCRIPTION:

A. Performance verification is an ongoing process and shall be performed throughout construction. Performance verification verifies that systems are operating in a manner consistent with the Construction Documents.

B. This Section covers specialty systems performance verification, as required to demonstrate that the equipment and systems of Section 28 10 00, Security Systems and Section 28 11 00, Video Surveillance Systems, are ready for safe and satisfactory operation, as defined by the Construction Documents. Performance verification shall include, but shall not be limited to, identification specialty system devices, cabling and equipment, cleaning, check-out, testing and adjusting of systems, preparation of equipment and systems documentation and of maintenance and operation manuals, Owner training, and preparation of record drawings.

C. Performance verification shall conclude with the completion of required testing, training, and system documentation as specified herein and required to demonstrate the proper operation of the specialty equipment and systems.

D. Security systems covered by this Section are Section 28 10 00, Security Systems, and Section 28 11 00, Video Surveillance Systems.

1.02 QUALITY ASSURANCE:

A. Provide a Security Systems Performance Verification Supervisor for the security systems. The Security Systems Performance Verification Supervisor shall have 10 years experience in security systems contracting. The Security Systems Performance Verification Supervisor shall become familiar with the Owner's project requirements and the requirements of the performance verification process as defined in this Section. The Security Systems Performance Verification Supervisor shall coordinate and execute the required performance verification activities.

B. The Security Systems Performance Verification Supervisor shall review submittal data for conformance with the requirements of the Project, shall monitor compliance with the requirements specified herein for storage and protection of equipment during construction, shall oversee testing, and shall document that the scheduled and specified performance requirements of each system have been accomplished.

1.03 PERFORMANCE VERIFICATION RESPONSIBILITIES:

A. The Security Systems Performance Verification Supervisor shall be responsible for scheduling, supervising, coordinating, and executing the testing and performance verification activities as specified herein.

B. Security systems performance verification shall take place in three phases. Performance verification requirements for each phase are as follows:

1. Construction Phase:

a. During the construction phase of the Project, transmit a status update report upon request to the Engineer (via e-mail), using the form included herein. (The Engineer will e-mail an electronic version of the attached form to the Contractor upon request.) The status update report shall include digital photographs of areas where significant progress has been made. Digital photographs shall be minimum 1200 x 1600 pixels in resolution. Both the detail in the report and the detail in the photographs shall be sufficient for the Engineer to assess the progress made to date, and respond appropriately to pay requests. Periods of inactivity will require only a retransmission of the most recent form (via e-mail), updated to reflect the new date, and that "no significant progress has been made since the last status report was submitted". Status reports will not be requested more than once every 2 weeks.

b. Provide documentation of installed systems and equipment and develop functional testing procedures, prior to normal operation and maintenance manual submittals. This documentation shall include detailed manufacturer installation, operating, troubleshooting and maintenance procedures; full factory testing reports, if any; and full warranty information, including responsibilities of the Owner to keep the warranty in force. In addition, the installation, check-out materials that are actually shipped inside the equipment, and the actual field check-out sheet forms to be used by the factory or field technicians shall be submitted to the Engineer.

c. Develop and submit to the Engineer for review and comment, prior to system functional testing, a complete functional testing plan using manufacturer's testing procedures and functional testing checklists for equipment to be commissioned.

d. Assist in clarifying the proposed operation and control of equipment in areas where the specifications, drawings or equipment documentation is not sufficient for writing detailed testing procedures.

e. Review the proposed functional test procedures to ensure feasibility, safety, and equipment protection. Obtain approval from the Engineer for proposed functional test procedures.

f. Prepare a preliminary schedule for performance verification activities, including equipment testing and adjusting from start to completion, and update the schedule during the construction period, as appropriate. Notify the Engineer immediately when performance verification activities not yet performed, or not yet scheduled, will delay construction.

g. Provide functional testing for equipment and execute the security systems related portions of the functional checklists of all the equipment during the testing process.

h. Perform and document functional tests results, providing a copy to the Engineer.

i. Correct noncompliance items before beginning acceptance testing. Discrepancies and problems shall be remedied before acceptance testing.

2. Acceptance Phase:

a. Place equipment and systems into operation and continue their operation during each working day of the acceptance testing and performance verification activities, as required.

b. Provide skilled technicians to execute acceptance testing of each system. Technicians shall be available and present during the agreed upon scheduled acceptance tests and for sufficient duration to complete the necessary tests, adjustments and problem-solving.

c. Perform acceptance testing for specified systems and equipment as directed by the Owner and interpret the test data as necessary.

d. Correct deficiencies (differences between specified and observed performance) as identified and interpreted by the Engineer and retest the equipment, as required to demonstrate proper operation and performance.

e. Prepare operation and maintenance manuals as specified, including clarifying and updating the original sequences of operation to as-built conditions.

f. Maintain marked-up record drawings and produce final record drawings of project drawings and contractor-generated coordination drawings.

g. Provide specified training of the Owner's operating personnel.

h. Coordinate with equipment manufacturers to determine specific requirements to maintain the validity of the warranty.

3. Warranty Period:

a. Correct deficiencies and make necessary adjustments to operations and maintenance manuals, and as-built drawings system or equipment modifications made during the warranty period.

PART 2: PRODUCTS

2.01 TEST EQUIPMENT:

A. Standard testing equipment required to perform the required testing shall be provided by the Contractor for the equipment or system being tested.

B. Test equipment shall be of the quality and accuracy required to test and/or measure system performance with the tolerances specified and shall have been calibrated within the last 12 months, or as specified herein. Equipment shall be calibrated according to the manufacturer's recommended intervals and when dropped or damaged. Calibration tags shall be affixed or certificates available on request. Accuracy of sensors shall be at least twice that of the instrumentation being tested.

PART 3: EXECUTION

3.01 SUBMITTALS:

A. Submit additional documentation as required to support the performance verification process. This additional submittal documentation shall include, at a minimum, the proposed functional testing plan, and functional testing checklists.

3.02 FUNCTIONAL TESTING:

A. General:

1. Functional testing shall be performed as required to ensure that the equipment and systems are properly installed and ready for operation, so that acceptance testing may proceed without delays. Follow the approved

functional testing procedures. Sampling strategies shall not be used for functional testing. The functional testing for equipment and subsystems of a given system shall be successfully completed and documented prior to acceptance testing of the system.

2. Functional testing plan: develop the detailed functional testing plans for equipment and systems that are to be commissioned, as specified herein. Review the proposed procedures and functional testing documentation to ensure that there is written documentation that each of the manufacturer-recommended procedures has been completed.

3. The functional testing plan shall include the manufacturer's standard written check-out procedures copied from the installation manuals and manufacturer's normally used field check-out sheets. The plan shall include checklists and procedures with specific boxes or lines for recording and documenting the tests recommended by the equipment manufacturer, and as specified herein. Each checklist shall include a summary statement with a signature block at the end of the plan.

B. Security Systems Tests:

1. Access Control and Alarm Monitoring Systems:

a. Program an access card for each of the following clearances:

1) Master access level to open all doors in the system.

2) Program a second access card to open all doors in the system, but then classify the card as lost or stolen to test stolen card used event.

3) Program an active access card with limited access to only main entry doors to test access denied events.

b. Attempt to access each door using the valid card first, and the card classified as lost or stolen card second and the limited

c. Confirm that a valid card read performs the actions specified herein and indicated on the Drawings.

d. Print a report showing the activity of the valid card during the test period, as well as the alarm activity for the test period. Confirm that the report shows a valid access for each door in the system for the valid card, and that the card classified as lost or stolen generated an appropriate alarm or exception report for each door in the system. Present this report to the Engineer.

e. For each access controlled door, the following alarm conditions shall be tested:

1) Door forced open. A card reader controlled door is opened without the use of a valid credential or an exit only monitored door is opened when armed.

2) Door held open alarm. Door held open longer that the predetermined allowed time after a valid entry or exit.

f. For each of the above alarm conditions, test that the appropriate ACAMS system event and message is displayed on the operator workstation.

g. Test each door alarm condition reporting to the Central Station when the IDS system is armed.

h. Test each duress button to report to the Central Station 24/7.

i. Print a report showing the alarm activity for the test period. Confirm that the report shows an alarm or exception appropriate for the zone and breach for each intrusion detection or duress alarm zone or device in the system. Present this report to the Engineer.

2. Video Surveillance Systems:

a. Display each camera in the system on the operator workstation monitor in color. Where day/night type cameras are implemented, display each camera in the daytime in color, and at nighttime in black and white. Record a minimum of 5 minutes of video from each camera in the system at a minimum of 7 frames per second, between the hours of 9:00 am and 5:00 pm. Record a minimum of 5 minutes of video from each camera in the system at a minimum of 7 frames per second, between the hours of 11:00 pm and 3:00 am.

b. Demonstrate each feature of the video surveillance system. Confirm that each feature functions as specified herein. Demonstrate that the appropriate video camera is switched to the designated alarm monitor and moved to its preset pan-tilt-zoom position at the initiation of each intrusion detection or duress alarm event, valid and invalid access card read, initiation of an intercom call, and other events as indicated on the Drawings.

c. Demonstrate that the video recording system is operational and recording the appropriate video camera at the initiation of each intrusion detection or duress alarm event, valid and invalid access card read, initiation of an intercom call, and other events as indicated on the Drawings.

3. Intercom Systems:

a. Confirm that each remote intercom station can connect and provide clear noise-free communications with the telephone system as specified herein and indicated on the Drawings.

4. Cable Testing:

a. General:

1) Applies to Category 6 cables.

2) Testing shall be accomplished using an Agilent Technologies, Fluke Networks, or Ideal Industries test instrument supporting an extended frequency range to 250 MHz.

3) Test 100% of the cabling links.

4) The tester shall support the following requirements:

a) Level III accuracy as defined in TIA/EIA 568-C-2012.

b) Digital with fault location capabilities.

c) Measure ELFEXT and Power Sum ELFEXT.

d) Distinguish external noise from NEXT.

5) Input the test results into the test instrument manufacturer's reporting software. Tabulate and analyze results to ensure cabling system meets requirements specified herein.

6) Document failed pairs or strands. Replace cable, then retest. Repeat procedure until cable passes requirements.

7) Upon completion provide a hard copy report in 3-ring binder and on CD-ROM for review and approval.

8) A representative of the Owner shall be invited to witness the field testing. The representative shall be notified of the start date of the testing phase at least 5 business days before testing commences.

b. Other Copper Cabling Testing:

1) Each pair of other copper cabling shall be tested.

c. Twisted pair cable testing shall include:

1) Cable length.

2) Continuity.

3) Proper connectivity.

4) Open pairs.

5) Short circuits.

6) Reversed pairs.

7) EMI noise induction.

8) Attenuation.

9) Near end cross talk.

d. Category 6 Testing:

1) Each category 6 outlet/cable shall be tested and certified in accordance with TIA/EIA 568-C-2009. Each pair shall be tested. A test cable shall be used at the test unit end. Testing shall occur in both directions.

2) Each category 6 cabling link shall be tested in accordance with the field test specifications defined in TIA/EIA 568-C-2012.

3) Category 6 cable wire map shall report pass if the wiring of each wire-pair is determined to be correct as defined in TIA/EIA 568-C-2012.

4) Category 6 cable length test result shall report measured length of each pair of a basic link and channel based on the propagation delay measurement and the average value for nominal velocity of propagation. The physical length of the link shall be calculated using the pair with the shortest electrical delay. This length figure shall be reported and shall be used for making the pass/fail decision. The pass/fail criteria are based on the maximum length allowed for the basic link configuration plus 10% to allow for the variation and uncertainty of the nominal velocity of propagation.

5) Category 6 cable near end crosstalk loss shall be tested for each wire pair combination from each end of the link (a total of 12 pair combinations). This parameter shall be measured from 1 MHz through 250 MHz with a maximum step size of 0.50 MHz. For a pass condition, the worst case NEXT margin and the worst value of NEXT shall be recorded for each case, the frequency at which it occurs, and the test limit value at this frequency.

6) Category 6 cable power sum near end crosstalk loss shall be evaluated and reported for each wire pair from both ends of the link under test (a total of 8 results). Evaluate this parameter from 1 MHz through 250 MHz with a maximum step size of 0.50 MHz. For a pass condition, the worst case PSNEXT margin and the worst PSNEXT value shall be recorded, the frequency at which it occurs, and the test limit value at this frequency.

7) Category 6 cable equal level far end crosstalk pair-to-pair loss shall be measured for each wire pair combination from both ends of the link under test. ELFEXT shall be measured from 1 MHz through 250 MHz with a maximum step size of 0.50 MHz. For a pass condition, the worst case ELFEXT margin and the worst ELFEXT value shall be recorded, the frequency at which it occurs, and the time limit value at this frequency.

8) Category 6 cable power sum equal level far end crosstalk loss shall be calculated by combining the effects of the

FEXT disturbance from 3 wire pairs on the fourth one. The test shall yield 8 wire pair combinations. Each wire pair shall be evaluated from 1 MHz through 250 MHz with a maximum step size of 0.50 MHz. For a pass condition, the worst case PSELFEXT margin and the worst PSELFEXT value shall be recorded, the frequency at which it occurs, and the test limit value at this frequency.

9) Category 6 cable return loss shall be measured from both ends of the link under test from 1 MHz through 250 MHz with a maximum step size of 0.50 MHz. For a pass condition, the worst case RL margin and the worst RL value shall be recorded, the frequency at which it occurs, and the test limit value at this frequency.

10) Category 6 cable attenuation-to-crosstalk ratio shall be calculated to determine the bandwidth for a two wire pair network in terms of signal-to-noise ratio. This calculation yields 12 combinations (6 from each end of the link). For a pass condition, the worst case ACR margin and the worst ACR value shall be recorded, the frequency at which it occurs, and the test limit value at this frequency.

3.03 ACCEPTANCE TESTING:

A. Before obtaining permission from the Owner to schedule the acceptance test, provide written certification that each system has been calibrated, tested and is ready to begin the 14-day burn-in period and acceptance testing.

B. Conduct final acceptance test after a period of not less than 14 consecutive normal working days of trouble- free operation.

C. During this burn-in period, each system shall operate continuously for 24 hours per day. During the acceptance test, demonstrate the correct operation of features and capabilities specified herein.

D. The Owner reserves the right to witness the acceptance tests. Notify the Owner at least 10 days prior to the date scheduled for the tests.

3.04 RETESTING OF EQUIPMENT AND/OR SYSTEMS:

A. Provide labor and materials required for retesting of any functional test found to be deficient.

B. Prior to retesting, submit required data indicating that the deficient items have been completed and/or corrected to the Engineer for approval and rescheduling of the functional test. If during the retesting it becomes apparent that the deficient items have not been completed and/or corrected as indicated in the data provided by the Contractor, the retesting shall be stopped. Costs for the performance verification team to further supervise the retesting of a functional test shall be the responsibility of the Contractor.

3.05 TESTING DOCUMENTATION, NONCONFORMANCE, AND APPROVALS:

A. Provide the Engineer with a list of outstanding items of the functional testing procedures that were not completed successfully within 2 days of test completion. The Engineer will then review the Contractor's functional testing reports and submit either a noncompliance report or an approval form to the Contractor. The Contractor shall work with the Engineer to retest deficiencies or uncompleted items. Correct items that are deficient or incomplete in the checklists and tests in a timely manner, and notify the Engineer as soon as outstanding items have been corrected. Resubmit an updated report and a statement of correction on the original noncompliance report. When requirements are completed, the Engineer will recommend approval of the functional testing of each system and schedule the acceptance testing of the equipment or system.

B. As acceptance testing progresses and deficiencies are identified, work with the Engineer to resolve the issues.

3.06 OPERATION AND MAINTENANCE DOCUMENTATION PACKAGE:

A. The Security Systems Performance Verification Supervisor shall compile and prepare documentation for equipment and systems covered in these Security Specifications and deliver this documentation for inclusion in the operation and maintenance manuals prior to the training of the Owner's personnel. The Engineer shall receive a copy of the operation and maintenance manuals for review.

3.07 INSTRUCTION OF OPERATING PERSONNEL:

A. The Security Systems Performance Verification Supervisor shall schedule, coordinate, assemble and deliver the documentation of the training required by these Security Specifications.

END OF SECTION 28 00 90

SECTION 28 10 00
SECURITY SYSTEMS

PART 1: GENERAL

1.01 DESCRIPTION:

1. This Section covers access control and alarm monitoring, and security related communications systems.

A. This Section covers wiring electric door hardware furnished and installed under Division 8.

B. Security systems general provisions are specified in Section 28 00 10, Security General.

C. Security systems performance verification is specified in Section 28 00 90, Security Performance Verification.

1.02 QUALITY ASSURANCE:

A. Installation of the alarm and access control system (ACAMS) shall be under the direct on-site supervision of a person or persons having completed the manufacturer's highest available certification program, and have direct field experience in the installation of a minimum three project of similar scope and size within the past 5 years. In addition the installation company shall have at the minimum two permanently employed persons with current system certification in their field office directly responsible for the installation and ongoing maintenance of the project. The office shall be located within 100 mile radius of the project.

B. All field technicians shall have completed as a minimum, the factory training recommended by the manufacturer of the system provided.

C. The installation company shall be a currently listed as an authorized dealer or business partner by the manufacturer of the system provided, and shall have been listed as such for a minimum of 3 years.

PART 2: PRODUCTS

2.01 GENERAL:

A. Tamper Provisions:

1. Enclosures, cabinets, housings, and boxes with hinged doors or removable covers which contain circuits of the access control system or intrusion detection system and its power supplies shall be provided with cover operated, corrosion-resistant tamper switches, arranged to initiate an alarm signal when the door or cover is moved as little as 0.25" from its normally closed position.

1. Pullboxes with covers secured with tamperproof screws or with spot welding shall not require tamper switches.

2.02 DETECTION DEVICES:

A. Magnetic Contacts:

1. For hinged doors: balanced 1" round recessed switches for door head installation. Switches shall be magnetic, double-pole, double-throw type, providing dual circuit operation, designed for line supervision. Switches shall be tested and proven capable of initiating an alarm signal when the protected door is opened 2" on the latch side.

2. For overhead doors: balanced switches, extra heavy duty, aluminum bar stock construction, floor-mounted contact, double-pole, double-throw type, providing dual circuit operation, for use on roll-up doors and rolling gates. Contacts shall have 3' stainless steel armored cables.

3. Alarm contacts shall be designed for 12 V to 30 V DC, non-polarized service.

B. Duress Devices:

1. Push-for-Help Buttons:

a. Designed for mounting under counter in single-gang box.

b. Latching LED call-placed indicator.

c. Tamperproof screws.

d. Manufacturer: Ademco, or Sentrol.

2.01 INTRUSION DETECTION SYSTEMS (IDS):

A. General:

1. Provide a microprocessor-based control/digital communicator that can provide intrusion, duress, and critical equipment monitoring. The system shall have a minimum of 48 individually addressable points that can transmit signals to a central station receiver. The system shall have the capability of controlling up to 16 outputs.

2. The system shall have arming stations with a touch pad through which users control security functions. Arming stations shall also have a minimum 16-character alphanumeric display. Displays shall show system status and give prompts to system operation. Arming stations shall display the status of 48 separate protection zones.

3. The system shall accommodate up to 4 8 microprocessor-based arming stations. All system operations shall be accomplished at any arming station.

B. Point programming: each of the points shall be programmable as to whether they are controlled versus 24 hours, interior versus perimeter, instant versus delayed, silent versus audible, and local or reporting. Additionally, each point shall be programmable to report to three separate telephone numbers.

C. Output Circuits:

1. Alarm power outputs: shall power audible alarms. Alarm circuits shall be supervised. There shall be 4 distinct audible patterns from which to select.

2. Additional relay outputs: capacity to expand to 16 additional relays. These relays shall be programmable to activate on alarms or other selected system events.

D. System Partitioning:

1. Point assignment: points shall be assignable to 1 of a minimum of 4 areas of protection.

2. Area arming: each area shall be separately armed and disarmed from any of the arming stations. Area 1 shall have the option of being a shared area that disarms automatically with the first area disarmed and arms automatically when the second area is armed. Alternately, area 1 can be a master area that cannot be armed until areas 2, 3, and 4 are armed.

E. Programming: system functions shall be programmable at the system site or remotely via the use of the dial-up telephone network. Minimum programmable system passcode shall be used to prevent unauthorized remote programming attempts. Telephone access to the system shall be a ring counter or user initiated access.

F. Remote keypads: shall allow arming and disarming of the system, shunting of individual zones, and adjusting any delay periods.

G. Digital communicators shall have the following minimum features:

1. Programmable delay before dialing.

2. Programmable dial attempts.

3. AC failure and AC restoral reporting.

4. Low battery and battery restoral reporting.

H. Manufacturer: Bosch, Digital Monitoring Products, or DSC by Tyco Security Electronics.

2.03 ACCESS CONTROL AND ALARM MONITORING SYSTEMS (ACAMS):

A. General:

1. The new access control and monitoring system (ACAMS) shall consist of head-end servers, a workstation and a hierarchy of access controllers that communicate utilizing a TCP/IP based Ethernet network. The system shall be capable of routing individual alarms to any selected workstation based on event type and time of day.

2. The system (hardware and software) shall support the quantity and types of devices specified herein and indicated on the Drawings, including software licenses for 1 user per workstation.

3. The system shall include sufficient processing capacity and speed and shall be configured to process valid access requests, and unlock the doors, within 1.5 s when all locations are attempted simultaneously.

4. The ACAMS shall be modular in nature, allowing system capacities to be easily expanded without the replacement (or rendering obsolete or non-usable) any hardware in the system or requiring major changes to system operation. All defined system data as well as historical information shall be maintained.

5. Provide the quantity and type of software licenses required to support the servers and workstations at the levels of functionality specified herein, and as indicated on the Drawings.

B. Access Control System Features:

1. Access control, alarm reporting and acknowledgement, alarm graphics, standard reports, photo badging, and video surveillance systems control shall be combined into a distributed control and management system.

2. Access control decisions shall be made by local panels utilizing their databases. Local panels shall report field events to the system workstations for display using a graphic user interface.

3. The ACAMS shall be an integrated system that utilizes a single, industry-standard relational database management system for the storage and manipulation of related data. The ACAMS shall include a server or network appliance controller/server with operating system and applications software, operator and administrator terminals with appropriate software, hard copy printers and fixed magnetic storage media.

4. The security devices shall communicate with the field panels via a dedicated cable network. The field panels shall communicate to the server via a Fast Ethernet 100/1000, TCP/IP network.

5. A client server architecture utilizing LINUX, or Microsoft Windows Server 2008 for the server operating system, and Windows 7 Professional or Windows 8 Professional for the client operating system.

6. The system shall validate cardholder credentials by use of downloaded personnel records, card formats, PINs, biometric enrollment and multiple active cards. The system shall compare the time, location, and unique credential number of an attempted entry with information stored in memory.

7. Access to a designated area will be validated only when a user’s credential has a valid number for its facility and the number is valid for the current time and for the reader where it is used.

8. The system shall access the hardware that validates the person and monitor the security of a building by use of controllers, doors, readers, elevators, inputs and outputs. When access has been validated, a signal to the door locking device shall be activated to enable alarm-free access at that location.

9. The system shall be configured by use of an administrative application, and shall provide configuration templates.

10. The system shall monitor access control activities by use of Monitor Station, Alarm configuration, video surveillance system, and dynamic graphical maps display of alarm, door, and event activity.

11. The system shall restrict administrative and monitoring station activity by use of privileges and authentication (user password) using Microsoft Windows Operating System Password Function and Windows Active Directory user access authentication.

12. The system shall report on various aspects of the system by use of reports (canned and configurable). Reports shall be able to exported to a PDF file or to a printer.

13. The system shall have the capability to report off-normal security device conditions both audibly and visually.

14. The system shall control hardware from the monitoring station by use of manual actions, events, and cause lists.

15. The system shall provide record and data management by use of historical archive and replay, full audit trail and automated and manual import and export (data and images).

16. The system shall allow for data to be imported from other products by use of database migration tools (card holder data and configuration data) from 3rd party applications via XML formatted data exchange.

C. Network resources:

1. DNS: The system shall support setting IP addresses for up to two domain name servers.

2. Email settings: The system shall support the use of email notifications of alarm events. The system user must setup the email server IP address or DNS name and the email address of the network controller. A network administrator must setup the network mail server to relay email for the IP address of the network controller.

3. NAS: The system shall support the use of network attached storage (NAS) devices for backups. The network administrator shall create a domain user account for the network controller and a password. The system user must configure the network attached storage in the system including the domain

name, server IP address, share name, and the directory where the network controller may store data.

4. Network Time Servers: The system shall support the use of network time servers to ensure that the network controller and its nodes will be regularly synchronized with the exact time used by all other network resources.

5. LDAP: It shall be possible to configure an Active Directory Server with the security management system to provide single user-login capability. Password rules and authentication will be governed by the LDAP server.

D. Application Software:

1. The access control system software shall serve as a database manager, controlling badge data, access rights, time schedules, multiple operation modes and alarm point information.

2. Database changes shall be downloaded from the system server to the field panels. The system server shall determine which changes are downloaded to which field panels based on the equipment connected to those panels.

3. The system shall not download all changes to all panels without regard to which doors are assigned to which panels.

4. Personnel records and cardholder management

a. The system shall generate and store up to 50000 personnel records.

b. The system shall allow a user to create personnel records either through the use of templates or directly input into the personnel record.

c. Each record shall be tabular in design and shall allow for multiple database tables per cardholder record.

d. The user shall have the ability to perform the following in personnel records:

1) Assign multiple cards to individual cardholders.

2) Enable or disable the cards.

3) Define an expiration date and time.

4) Define default expiration dates based on card types.

5) Define the acceptable card type.

6) Define the card number, site code, and PIN.

7) Mark the card as lost, stolen, or deactivated.

8) Issue temporary or restore permanent cards.

9) Display the employee photo image and/or signature.

10) Create, edit, or delete the cardholder's access privileges and additional personnel attributes.

e. The selection of card type shall include ABA formats, Wiegand formats, and smart card formats.

f. The personnel records shall provide multiple pages of personnel data containing default system and user-defined fields. Labels for user-defined field tabs shall be customizable by the System Administrator with the appropriate privileges. Each user-defined field shall allow a name, description and label.

g. User-defined fields shall be definable as Mandatory or Unique.

h. User-defined fields shall support masking to provide consistency of data entry across all system operators. Custom masks, as well as predefined masks, shall be available:

i. The ACAMS shall support user-defined personnel views. Personnel views shall provide the ability to customize the personnel record by adding and/or removing certain objects from the operator’s view. Personnel views shall be assignable to ACAMS operators via the operator’s assigned privilege and shall be definable for use in the creation and/or editing of the personnel record. All personnel views enabled for an operator shall be selectable from the current view to allow an operator to switch views in real time.

5. Access Rights:

a. The software shall allow for assignment of the access rights to cardholders.

b. The access right shall allow the administrator to restrict where the cardholder may go and when they may go there.

c. Each cardholder shall be allowed multiple access rights and multiple badges.

d. Each access right may be assigned a different schedule.

e. Software shall automatically load the proper access rights into the proper field panels automatically without operator intervention.

f. Templates shall be available on the system to assist the operator in assigning rights during the badging process.

6. Password Protection:

a. The software shall provide password protection of workstations and servers.

b. Permissions shall be assigned to users to allow the following minimum restriction levels:

1) View only.

2) Edit/update cardholders.

3) Edit/update system configuration.

7. Reports:

a. The SMS shall provide configurable data reports for database configuration, historical activity (Journal) and audit tracking. Pre-defined reports shall be available for download and import into the system.

b. The operator shall not have to use SQL command language to generate standard reports.

c. The report function at the minimum shall perform the following:

1) Create reports about any object.

2) Create report templates to simplify report design.

3) Run reports on demand.

4) Save report results for sharing between different users of the application.

5) Export reports into formats such as PDF, RTF, TXT, or Excel (XLS).

6) Specify a query to select and filter the records on which to report.

7) Specify the data fields to be included in a report.

8) Specify a design for the report layout.

9) Design a report form to be used as a layout for headers / footers for multiple reports.

10) Access and use system pre-defined report forms.

11) Select tabular, multi-line, or free form report layouts.

12) Report on objects linked together with parent / child relations.

13) Schedule reports to run automatically on a customized schedule.

14) Send exported report files to the printer or to external recipients via e-mail.

d. It shall be possible to use third party report tools, such as Crystal Reports, to generate reports.

8. Import / Export:

a. The ACAMS 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.

b. The system shall also support importing from CSV files.

c. The ACAMS shall provide an automated import mechanism. 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.

d. The ACAMS shall have the capability to perform automated imports from an Open Database Connectivity (ODBC) data source allowing the import of personnel data directly into the system database.

e. The system shall have the ability to connect to a directory service source via the Lightweight Directory Application Protocol (LDAP). The connection to the LDAP source shall be user-configurable directly from the ACAMS and shall not require custom code. The LDAP interface shall also support the automatic assignment of ACAMS clearances based on data contained in the LDAP record. The LDAP feature shall support the following features:

1) LDAP server name and user-defined port number.

2) A base distinguished name for the root of searches.

3) A user-definable LDAP search filter to refine object search.

4) User-defined mapping of attributes to ACAMS personnel fields.

5) The use of a Distinguished Name (DN) entry for the ACAMS to authenticate to LDAP.

6) Option to search all sub-levels of the directory from the base DN.

7) Preview sample-data based on ACAMS LDAP import settings.

8) Automatic roles-based ACAMS clearance(s) based on two fields of source data.

9) Automatic import of directory entries from the LDAP source.

10) Authentication via a user-definable LDAP user account and SSL.

11) Automatic ACAMS clearance assignment.

9. Holidays:

a. The system shall support the creation of schedules that designate individual days as holidays, or special days to cover vacations, maintenance shutdowns, or other events, indefinitely into the future. Holidays or special days can signal that the system shall operate on a schedule different from the normal schedule.

b. The system shall not limit the number of holidays.

10. Area Control:

a. The system shall permit area control in the following 5 ways:

1) Hard anti-passback: the hard anti-passback feature shall require that a badge always be used to enter and exit an area. The system shall allow supervisors whose cards are configured as such be exempt from this feature as configured by the system administrator.

2) Soft anti-passback: the soft anti-passback feature shall require that a badge be used to enter and exit and area, but access shall not be denied if the badge was not presented in the correct order. The system shall generate a pass-back alarm. The system shall allow supervisors whose cards are configured as such be exempt from this feature as configured by the system administrator.

3) Timed anti-passback: the timed anti-passback feature shall allow the system administrator to decide how long after a cardholder has swiped will they have to wait before the same card will be accepted again at the same reader, or globally at any other reader defined in the area.

4) Multiple man rule: multiple man rule shall be provided to restrict access to an area unless there is more than one cardholder present. Individual exit shall be permitted until the required number of people who originally gain access is reached, at which point the multiple man rule applies for exiting.

5) Occupancy limits: occupancy limit shall restrict the number of cardholders that will be present in an area at any given time. Occupancy limits shall be able to be defined by the systems administrator for each controlled area.

11. Video Surveillance System Interface:

a. The software shall interface to the proposed video surveillance system head-end via a software level interface to allow control by the access control system.

b. Video surveillance system interface shall support the following functions:

 1) Camera call up pan-tilt-zoom positioning and displaying camera images on a pre-designated monitor or monitor segment on the video surveillance system workstation.

 2) Automatically or on-demand display camera images on the ACAMS monitoring display or web client.

 3) Automatic tagging of the recorded video clip in the video surveillance system recording with the ACAMS alarm data link to allow retrieval of alarm related video during historical data search and replay.

 4) Automatic activation of recording on ACAMS alarm events.

 5) Allow operator to view live video and playback of recorded video from the video surveillance system and IP cameras. The software shall allow instant replay of recently recorded video from any digital video source.

c. It shall be possible to recall and replay stored video clips associated with the selected alarm using the alarms management screen.

d. The video functions (live video display, instant replay of recently recorded video, playback of stored video, and configuration of the video functions) shall be available to any operator (with appropriate privileges) on any workstation connected to the system.

e. System shall provide through the graphical map interface a simple means for a guard or other operator to quickly initiate recording on a specific camera (if it were not otherwise recording).

f. The system shall provide a video playback of alarm related video on the ACAMS workstation.

g. The system shall limit operator access to video based on individual permissions.

h. Events received from Access Control, or others shall be capable of triggering video recording, to stop video recording and to display video playback.

12. Manual Access Control Panel Control:

a. The software shall support manual control of output points, and manual override of schedules.

b. The software shall require a descriptive explanation for manual override command from a workstation if required by the system administrator.

13. Global Data Exchange:

a. The system shall provide global data exchange. Any input point in the system shall be permitted to permit activation of any output point such as a relay that opens a door or sound an alarm regardless of the specific field panel or controller to which the input and output points are attached.

b. The system shall be able to arm/disarm global data exchange individually on a schedule.

14. Double Card Unlock:

a. The system shall support the use of a Double Card Presentation mode. This mode shall allow the presentation of a card twice in quick succession at a designated reader. Such a "double read" shall change the locked portal to an unlocked state until a subsequent relock event or user-designated timeout occurs.

b. The double card presentation mode shall be enabled on an individual portal basis and shall also require a designation on the access level assigned to the cardholder.

c. The mode shall adhere to time spec and threat level restrictions.

15. Keypad timed unlock:

a. It shall be possible to enable a timed unlock feature for a portal that has a combination reader/keypad device. Once this feature is enabled, any cardholder with valid access to the portal shall be able to specify how long the portal will remain unlocked.

b. A cardholder presents his or her card and then enters the associated PIN, followed by the appropriate command to unlock the door.

c. The portal will remain unlocked for the specified number of minutes, unless it is closed before the timer expires. If the portal remains open after the timer has expired, a [Door Held Open] alarm will be activated.

d. If reader/keypad devices are located on both sides of the portal, cardholders will be able to use either device to initiate a timed unlock.

16. Guard Tour Option:

a. This feature shall allow Guard Tour patrol sequences to be created consisting of a number of designated clocking points, which the patrolling guard has to visit.

b. A guard tour sequence shall define the order in which the clocking points are to be visited and also how long the guard should take to move between each clocking point location. A window of tolerance shall be included to add a +/- value to these timings.

c. The system operator shall initiate the required guard tour patrol and declares the guard who is to undertake the tour of the premises. The system shall then automatically monitor the guards progress around the patrol tour, reporting alarms if the clocking points are either out of sequence, or the guard arrives too early, or becomes overdue. The operator shall be notified as each point is clocked to allow the guard’s progress around the site to be monitored. A patrol tour shall be able to be suspended, if required, and will automatically resume when the next point is then clocked.

d. Guard tour patrols shall be configurable on a per company basis when multiple companies are required on a site. Management reports shall be created from the history log to confirm when each guard tour was carried out, including any deviations or incidents during the tour.

17. Threat Levels:

a. It shall be possible to alter security system behavior through the use of threat levels. Groups of threat levels may be created and assigned to portal groups, access levels, input groups, output groups, floor groups, and event actions. The behavior of groups, access levels, and event actions with assigned threat level groups shall change based upon the current system threat level.

b. The security management system shall support 32 threat level groups.

c. It shall also be possible to change the system threat level in response to an alarm event.

d. The current system threat level shall display in the title bar of the security application interface and on floor plans.

18. Alarm Management:

a. The software shall be capable of accepting alarms directly from controllers, or generating alarms based on polling of data in controllers and comparing to limits or conditional equations configured through the software. Any alarm (regardless of its origination) shall be integrated into the overall alarm management system and shall appear in standard alarm reports, be available for user acknowledgment, and have the option of displaying graphics, or reports. Alarm management features shall include:

1) Automatic logging in the database of the alarm message, time stamp, user name, time of acknowledgement, and time of alarm silence.

2) Automatic printing of the alarm information or alarm report to an alarm printer or report printer. This feature shall be disabled upon initial system installation.

3) Sounding of an audible beep or playing an audio (.wav) file.

4) Sending an e-mail or alphanumeric page to anyone listed in a workstation e-mail account address.

5) An alarm viewer shall be included to display the following information:

a) Date/time of alarm.

b) Name of alarm.

c) Priority of alarm.

d) Alarm message.

e) User text input.

f) Acknowledged by.

g) Data/time of acknowledgement.

6) The operator shall have the ability to highlight a specific alarm and select a button or click to display an associated graphic map.

7) The system shall automatically display graphic maps indicating status of input points and display the real time status of output points.

19. E-mail Alarms:

a. The ACAMS shall support the ability to automatically e-mail alarm condition messages.

b. Each alarm definition shall allow a destination e-mail address to be defined. The e-mail address may be an address group as defined in the e-mail MAPI application.

c. E-mail alarm messages shall be controlled by time of day and day of the week.

20. Support for Intrusion Detection System (IDS) Integration:

a. The ACAMS shall support a high-level (serial or network interface) to an intrusion detection system (IDS).

b. The integration to the IDS shall support, at a minimum, secondary monitoring of all ACAMS alarm transactions to be monitored by a central station, if desired.

c. The IDS integration shall also include the ability to arm and disarm the IDS from the ACAMS user interface.

d. The communication with the IDS control panel shall be monitored, and the ACAMS shall produce an alarm in the event of a communications failure.

21. Remote lockset integration:

1) The system shall support the integration of Wi-Fi enabled locksets with the security management system.

2) Once a lockset is installed and registered with the controller, it appears in the security application as a "Remote Lockset" node, which can be enabled and configured to work with the controller.

3) It shall be possible to set configuration options for a remote lockset to change its call-in and lockout behaviors.

4) It shall be possible to configure the reader and portal that were automatically created for a remote lockset.

5) It shall be possible to view cached information for a remote lockset, for troubleshooting purposes.

6) It shall be possible to specify special-use formats for access cards to be used with remote locksets.

7) The remote lockset shall be able to send high priority events to the controller.

8) The remote lockset shall update the controller with the current voltage level of its battery upon each connection.

9) It shall be possible to schedule an automatic unlock period for remote-lockset portals. The start of this period can be triggered by time or by an initial valid card read.

22. System Partitioning:

a. The ACAMS shall allow system administrators to separate the creation and viewing of objects into partitions. ACAMS operators shall be associated with partitions and this shall determine which objects operators have the ability to create and or view. The ACAMS shall support an unlimited number of partitions.

b. The ACAMS partitions shall include but not be limited to the following objects:

1) Personnel

2) Clearances

3) Doors

4) Controllers with all associated hardware (readers, inputs, outputs, etc)

5) Video servers with all associated objects (cameras, tours, views, etc)

6) Application layouts
7) Events

8) Dynamic views

9) Maps

10) Reports, forms, results

11) Holidays

12) Badge layouts

13) Queries

14) Images

c. Through the use of privileges, the ACAMS System Administrator shall be able to determine which objects are associated with a particular partition. These objects shall then be assigned to System Operators with the appropriate privilege.

d. The ACAMS shall support a super-user assigned the ‘System All’ privilege who shall have full access to all objects in all partitions.

e. Any operator shall have the ability to be assigned access rights to any partition. Individual Access rights shall be created and have the ability to be assigned to any users of the ACAMS.

f. The ACAMS shall allow objects to be created in any partition. The ACAMS shall have the ability to grant or remove permission from any object in any partition.

g. The ACAMS shall provide the ability to move objects from one partition to another partition without the requirement of deleting and recreating.

h. The ACAMS shall support the display of all associated objects contained within a partition.

23. Monitoring Operator Interface / Activity Monitoring:

a. The ACAMS shall contain a monitoring component that is capable of displaying the current state of any object in the system. Additionally the monitoring station shall be capable of displaying a log of all activity that occurs in the system, from object state changes, to access control information. All text for events (alarms) in the system shall be configurable to be displayed in color based on the user-specified priority of the event.

b. The Monitoring Station shall be capable of showing all changes occurring to an object without requiring the associated activity messages for that object to be routed to that monitoring station. The ACAMS shall require the operator to have appropriate permissions to view and/or control any object.

c. The monitoring station interface shall be user-customizable. The ACAMS shall support the ability of the end user to create a customized application layout for the monitoring station. The monitoring station shall support multiple application layouts that can be assigned to the operators. Each application layout can have multiple panes in the same window. Each pane shall have the ability to be moved to a specific screen.

d. The ACAMS shall provide the Operator with following functional capabilities:

1) Shall provide a scrolling list of lines showing current activity on the system.

2) Shall display activity in real-time as data is being transmitted by field hardware.

3) Shall include icons that indicate the type of activity and textual description of the activity.

4) A series of menus, driven by drop-down or trees, shall allow the Monitoring Station operator to perform manual actions, such as “momentary door unlock” for a given door.

5) As part of the manual action capability, the system shall provide screens or boxes that query the operator on specifics.

6) Ability to view a sortable list of active alarms or events and recently active alarms or activity.

7) Ability to view video from live or recorded view of cameras within the same GUI. The video screen GUI shall have on-screen camera controls providing PTZ control of individual cameras.

8) Objects shall be displayed to the operator based on his/her assigned operator privilege. The operator shall only be able to monitor/command those objects for which he or she has been assigned privilege.

9) When an operator logs out of a workstation and a new operator logs on, the objects displayed on the workstation screen shall by dynamically updated to display only those objects for which the new operator has privilege.

10) Allow the customization of columns as defined by the operator privilege.

11) Support multiple panes for the display of events, activities, video, personnel images, and maps.

12) Support the ability to attach a log message to an event, even after the event has been acknowledged.

13) Provide the ability to attach Predefined Log Messages to an event upon acknowledgement.

14) The ACAMS shall support audible alarm annunciation at operator workstations (operator configurable audio [WAV] files associated with alarms).

24. Graphic Maps

a. The ACAMS shall support graphic maps and icons to be displayed on the operator workstation monitor.

b. The system shall support an operator-programmable, color graphic map display that:

1) Shall be capable of showing the floor plan, the location of alarm devices, and alarm instructions for a facility.

2) Shall be centralized in the system configuration and displayed on the operators' workstations.

3) Shall allow various maps to be associated with different areas to create a hierarchy of maps.

4) Shall support graphic maps having a resolution of 1024x768 Pixels or greater.

c. Operators shall be able to use drag-and-drop operation to place dynamic system level object icons of all objects such as: cameras, video servers, inputs/outputs, events, maps, reports, dynamic views, and door/elevator icons. These dynamic object icons shall allow a system operator to perform tasks and issue commands related to the object by double-clicking on the icon.

d. The ACAMS shall allow the addition of new layers to the drawing (such that if the drawing must ever be reloaded due to an update of the drawing, the layer(s) created within the ACAMS will be added back automatically without additional reconfiguration).

e. The ACAMS shall be able to directly import the following file formats for the map:

1) AutoCAD (.DWG)

2) DXF

3) Windows Meta File (WMF)

4) TIFF (.TIF)

5) JPEG (.JPG)

6) PNG

7) Windows Bitmap (.BMP)

8) GIF

f. The Maps feature shall include two operational modes:

g. An administrative mode to allow configuring of the facility floor plans or site plans that show exterior features.

h. A runtime mode to allow monitoring and interacting with the configured facility layouts or site plans.

25. Web/Thin Client:

a. The ACAMS shall support a Thin Client to provide remote access to the ACAMS Server via a web browser. The Thin Client shall support Microsoft® Internet Explorer 9.0 or greater, Mozilla Firefox® 4.0 or greater or Google Chrome. The Thin Client shall support 128-bit AES encryption to the ACAMS Server.

b. The Thin Client shall support Single Sign-on utilizing Windows Authentication. The privileges of the ACAMS operator shall be propagated to the Thin Client User allowing only access to Security Objects for which the ACAMS Operator is authorized. The Thin Client shall provide support for Partitioning of the system and utilize the Partitions assigned to the Operator.

c. All changes made to the ACAMS database via the Thin Client shall be recorded in the Audit Trail Database.

d. The Thin Client shall provide Personnel Management, allowing the Operator to create and modify Personnel data (includes adding/removing clearances, schedules, and expiration dates). The Operator shall have the ability to enable and disable cards. The Operator shall have the ability to search for, edit, add, and delete Personnel records from the ACAMS database. The search function shall allow wildcards and shall include First name, Last name, card number, and user defined text 1.

e. The Thin Client shall support an Activity Monitor to provide a scrolling display of system activity. Activity shall be restricted based upon the Operator’s Privilege and Partition assignments.

Display controls shall include page up, page down, and a freeze function.

f. The Thin Client shall support Manual Actions to include the Locking/unlocking of doors, and the Activation/deactivation of events.

g. The Thin Client shall support the display of Dynamic Views as defined by the ACAMS. Dynamic Views shall provide a real time view of ACAMS data including Journal and Audit Trail history. Viewing of Multiple Dynamic Views shall be supported.

h. The Thin Client shall support creating, configuring, loading and saving of reports. Reports shall consist of personnel history activity or audit data. The report data shall allow sorting within the thin Client view page by any displayed field in ascending or descending order. The Thin Client shall allow reports to be saved in the following formats: XLS, CSV, XML, TXT or PDF. The operator shall have the option to save the report to a file or send it via email.

i. The Thin Client shall support Manual Action Challenges. The Manual Action Challenge shall require an operator to enter their login credentials (User name and password) when executing a manual action, such as a door unlock, from within the Thin client.

j. The Thin Client shall support the ability to query on a specific cardholder or a group of cardholders for the purpose of assigning clearances to multiple cardholders at once. Once the query is complete, the operator shall have the ability to assign a single access clearance or a group of clearances to all cardholders.

k. The Thin Client shall support the ability to display a door activity report from the web client cardholder record configuration view. In addition, it shall provide the ability to display the Activation / Expiration Date and Time for each credential assigned to a cardholder. The thin client shall display all user-defined personnel fields and the details of each assigned access clearance in a separate window.

l. The Thin Client shall support Auto-Logoff based upon inactivity. The Thin Client shall monitor user activity and shall automatically log a user out of the workstation after a user defined timeout period.

E. System Hardware:

1. File Server Minimum Requirements:

    a. Processors: Intel Xeon quad core 2.8 GHz.

    b. RAM: 4 GB of SDRAM.

    c. Controllers: SCSI-3 or SATA II Raid-5 controllers.

    d. Internal storage: Three 250 GB 7500 RPM SATA II hot-plug hard drives in a Raid-5 configuration.

    e. Optical drive: DVD-R/W drive.

    f. Network card: 10/100/1000Base-T.

    g. Monitors: 17" color LCD with integrated KVM and slide-away rack mount kit as specified in section 28 11 00 - Video Surveillance Systems.

    h. Redundant power supplies.

    i. Other components required for a complete and operational system, including mouse and keyboard.

    j. Servers shall meet the system manufacturer's recommendations where the system manufacturer's recommendations exceed these requirements.

2. Workstation (Client) Minimum Requirements:

    a. Processors: Intel Core i3 3.30 GHz, 3220M CPU.

    b. RAM: 4 GB DDR3, 1333 MHz.

    c. Controller: SATA II controller.

    d. Internal storage: 500 GB hard drive, 7200 rpm SATA.

    e. Optical drive: DVD-R/W drive.

    f. Network card: 10/100/1000Base-T.

    g. Monitor: 22" color LED flat panel monitor.

h. Other components required for a complete and operational system, including mouse and keyboard.

i. Workstations shall meet the system manufacturer's recommendations where the system manufacturer's recommendations exceed these requirements.

3. Access control panels:

a. Distributed intelligence architecture with each controller operating independently.

b. Database information shall be stored at the panel level. Decision making shall be performed at the field panel and upon loss of power the panel shall not revert to a degraded mode.

c. In the event of communications failure with the host, the controller shall provide complete control, operation and supervision of monitored and controlled points. In the communications failure mode the system shall store transactions in a first-in first-out buffer until the panel is brought back online at which time the data shall be uploaded to the server. The panel shall not revert to a degraded mode.

d. Field panels shall be flash ROM upgradeable.

e. Field panels shall support communications via TCP/IP, RS-232, RS-485, TCP/IP, and dial-up modems.

f. Field panels shall hold a minimum of 10,000 cardholders in memory.

g. Field panels shall be mounted inside factory-provided equipment enclosures with key-lockable doors and tamper switches.

h. Field panels shall be provided with a UPS sized to provide 24 hours of uninterrupted power to the controller.

i. Communications lines to the host shall be supervised. In the event of failure, the system shall detect failure within 2 s and report the failure as an alarm condition.

j. Loss of primary power failure shall result in alarm condition.

k. Field panels shall report cabinet tamper, reader communications loss, AC power loss, and low battery.

4. Single Door (PoE) Edge Network Controller:

a. The intelligent single door PoE edge network controller shall provide access control processing, host functionality and power for a single door, including reader, lock, door status, request-to-exit device and auxiliary sounder.

b. Each intelligent controller can be powered using PoE or locally via a 12VDC supply. When powered using PoE, up to 700mA shall be available for reader and electric lock power.

c. The network door controller shall provide full distributed processing of all access control functions. Each controller shall provide distributed intelligence and fast response to access requests including a minimum memory capacity of 50,000 cardholders and 10,500 offline event transactions.

d. The controller shall support Flash Memory firmware architecture for ease of updating.

5. The controller shall support Wiegand output card readers or smart card readers.

6. The Edge Network Controller shall provide onboard connections to a ACAMS controller or server via the Local or Wide Area Network.

7. The ACAMS shall provide direct network discovery and programming for the Edge Network Controller for simplified installation.

8. The controller shall be UL listed and conform to UL standards for access control systems.

F. Identification badge system: The access control and alarm monitoring system shall include an integrated video imaging and photo ID system with the following capabilities and components:

1. The video imaging and photo ID system shall share a common database with the access control system such that data has to be entered only once. Data shall be automatically downloaded to the system main and back-up servers.

2. The system shall be interfaced to the video surveillance system at each remote site such that the video surveillance system shall transmit a video image from the associated video camera in the event of a security alarm at an entry door. When the alarm is due to the use of an unauthorized or invalid card, the system shall also display a photo ID image from the database for comparison with the video image.

3. The identification badging system shall store a minimum of 65,000 cardholder images on hard disk. Stored images shall be displayed upon request.

4. Custom card backgrounds shall be displayed upon request.

5. Badge Design and Printing:

   a. A comprehensive integrated badge design facility shall be provided as a standard feature of the software, with no separate licenses or license fees required to activate the feature. The badge designer must allow an unrestricted number of custom badge layouts to be defined then saved with a suitable description as a reference. This shall make full use of the card record details such as name, card number, inactive date as well as allowing personal data to be included in the badge design. Company logos shall be imported as bitmaps (BMP) or JPEG images to provide a personalized corporate appearance to the card.

   b. All elements incorporated into the design shall be able to be rotated.

   c. Each badge design shall contain either a single sided design or a double-sided design. Each side of the card shall also be designated as being blank, or magnetic stripe side, or smart chip side, to ensure the designer is aware of the available space where printing may be incorporated for each card combination. The badge designer function shall be capable of supporting portrait, landscape as well as standard and custom-sized card designs.

   d. When creating a new card record a badge preview screen shall also be included that displays the specific card's details on the selected badge design to allow confirmation prior to requesting the badge to be printed.

   e. Each new cardholder record shall have the option to be flagged for future printing. Cards flagged in this manner shall be easily recalled at a later stage and processed for output to the printer in a single action. Selecting multiple cards for bulk printing shall also allow each card to be printed either with its specific badge design, as defined within each card's record, or alternatively printed with a selected common badge design. Encoding of magnetic stripe cards shall also be included as part of the bulk printing process.

f. The ACAMS shall support any manufacturer's ID badge printer with a Microsoft Windows (depending on the workstation configuration) compatible printer driver.

g. The ACAMS shall provide the option to encode a magstripe card during the print cycle shall also be incorporated. Applications that require on-site encoding can combine both actions in a single process. Encoding may only be supported on a limited set of printer models defined by the ACAMS manufacturer.

h. Each badge design shall include a default printer, validity period, and access rights.

i. Objects (images, or other fields to be printed to the card) shall support the ability to be enabled or disabled by the presence of a specific label in the cardholder record. For instance, a logo indicating a certain training would be printed only if the personal data field identified indicated such a certification for that cardholder. Solutions requiring a separate badge design for any change in badge graphical content shall not be acceptable.

6. The badging system shall include the following components:

a. System hardware and software.

b. A portable USB digital camera with tripod, compatible with the video imaging and photo ID system, and a light source (as recommended by the system manufacturer) with stand.

c. Print ribbons, badges, a slot punch, and clips as required to print 500 badges.

d. Automatic card punch, one for each printer required.

7. Card printer: provide card printer meeting the following minimum requirements:

a. Process: dye sublimation with a clear coat printed over badge graphics.

b. Feed: automatic card feeder.

c. Encoding: inline encoding, conforming with badge encoding requirements.

d. Print speed: 1 min per card or faster.

e. Capability shall be provided to allow the operator to choose:

1) To print the currently displayed image.

2) To reshoot the picture without printing.

3) To store up to 1,000 images before printing.

8. Provide garment clips compatible with the cards selected.

G. Manufacturer: AMAG Technology Symmetry V7, Software House C·CURE 9000, or LENEL OnGuard.

2.04 ACCESS CONTROL PERIPHERAL EQUIPMENT:

A. Read Only Multi-technology Contactless Smart Card reader

1. Multi-technology contactless smart card reader shall read access control data from both 125 kHz and 13.56 MHz contactless smart cards. The multi-technology contactless smart card reader shall be designed for use in access control applications that require reading both 125 kHz Proximity and 13.56 MHz contactless smart cards by providing:

2. Unique read selection that enables iCLASS, proximity, or both technologies at the same time.

3. Guaranteed compatibility to read all HID data formats ensuring card-to-reader interoperability in multi-location installations and multi-card/reader populations when used with Genuine HID products.

4. Secure access control data exchange between the smart card and the reader utilizing key diversification and mutual authentication routines.
5. Compatible with the access control system provided.

6. The ability to read expanded smart card data format lengths up to 144 bits.

7. Backwards compatibility with legacy 125 KHz proximity access control formats (E.g. 26-bit, 32, 35-bit, 37-bit, 56-bit, and HID Corporate 1000 formats).

8. Product construction suitable for both indoor and outdoor applications.

9. Customizable behavior for indicator lights and audible tones.

10. Multi-technology contactless smart card reader shall comply with the following 13.56MHz-related standards to ensure product compatibility and predictability of performance:

    a. ISO 15693
    b. ISO 14443A
    c. ISO 14443B.

11. Contactless smart card reader shall be configurable to read 13.56 MHz data simultaneously from one to, at minimum, two of the following cards:

    a. HID iCLASS Access Control Sector/Application data

    b. ISO 15693 card serial number (CSN)

    c. ISO 14443A card serial number (CSN): including MIFARE & DESFire

    d. ISO 14443B card serial number (CSN)

12. Reader types as indicated on the drawings:

    a. Standard readers: surface-mounted style, contactless smart card readers designed for mounting into a single-gang back box.

    b. Mullion readers: surface-mounted style, contactless smart card readers designed for minimal space mounting configurations (mounting onto window and door mullions).

    c. Combination readers: surface-mounted style, contactless smart card readers and keypads integrated, designed for mounting into a single-gang box.

13. Contactless smart card readers shall provide priority processing for reading multi-technology (13.56 MHz & 125 kHz) credentials. When reading a multi-technology credential, the reader shall provide a selectable

priority of which technology to process and transmit data to the access control system.

14. The contactless smart card reader shall provide the ability to read card access data stored in the secure access control sector/application area of the ISO 15693 HID iCLASS card.

15. The contactless smart card reader shall be configurable to provide multiple hierarchical degrees of key compatibility for accessing the smart card access control data. Compatibility shall be provided for the following key structure options:

    a. Compatibility with higher security HID managed ELITE keys which provide a site-specific, unique, protected key structure.

    b. Compatibility with high security user-managed custom keys.

16. The contactless smart card reader shall be configurable to provide compatibility with all HID Prox formats, including Corporate 1000 and Long formats, or Indala Prox formats, including full support of any FlexPass® and FlexSecure® formats.

17. Contactless smart card reader shall be compatible with HID's iCLASS mutual authentication algorithm using 64-bit authentication keys. All RF data transmission between the card and reader shall encrypted using a secure algorithm to ensure that the communication between the card and reader can never be copied and repeated back to the reader (sniffing and replay).

18. Contactless smart card reader shall allow the reader firmware to be upgraded in the field without the need to remove the reader from the wall through the use of factory-provided Application

19. Cards.Readers shall be of potted, polycarbonate material, sealed to a NEMA 4X or IP65 rating.

20. Readers shall provide the ability to change operational features in the field through the use of a factory-programmed command card. Additionally, firmware shall be updatable by flashing the reader. Command card operational options shall include:

    a. Output configurations.
    b. LED and audio configuration.

    c. Keypad configurations.

21. Contactless smart card readers shall provide the following programmable audio-visual indication:

    a. An audio transducer shall provide various tone sequences to signify: access granted, access denied, power up, and diagnostics.

    b. A high-intensity light bar shall provide clear visual status (red/green/amber) that is visible even in bright sunlight.

    c. Contactless smart card read range shall be 2" to 3" using cards, 1" using key fobs, 1" using stickers (tags), 1" to 1.5" using smart + HID 125 kHz proximity cards, and 1" to 2" using MIFARE cards (card serial number only).

22. Contactless smart card reader shall provide the ability to transmit an alarm signal via and integrated optical tamper switch if an attempt is made to remove the reader from the wall. The tamper switch shall be programmable to provide a selectable action to provide a selectable action compatible with various tamper communication schemes provided by access control panel manufacturers.

23. Color: Black

24. Manufacturer: HID Multiclass Series.

B. Cards and RFID Tags:

1. Access cards: complete with photo identification pouch and garment clip, and slot punch and strap as approved by the Owner.

    a. Contactless smart cards: HID iClass 2001 16 kbit proximity car

    b. Provide custom printing on 1 side.

    c. Quantity: 200

C. Other Access Control Related Hardware:

1. Request-to-Exit Push Buttons:

    a. Single-gang box mounting.
    b. Normally open/normally closed, 1 A rated contacts.

    c. Illuminated push button.

d. Tamperproof mounting screws.

e. Access and secure LEDs integral with the faceplate or the push button.

f. Coverplate finish to match others in room.

g. Time delay module in compliance with NFPA 101-2009.

h. Manufacturer: Dortronics N or W series, Locknetics 700 series, or Securitron PB series.

D. Cabling: manufacturer's recommended type.

E. Miscellaneous Equipment:

a. Access card printer cartridges and supplies as required to print 1000 access cards.

b. Interface cables.

F. Request-to-Exit Motion Detectors:

1. Passive infrared type.

a. Walk-test light.

b. Form C, double-pole double-throw output relay rated for 30 V (AC/DC), 0.5 A.

c. UL listed.

d. Power: 12 V to 24 VDC.

e. Manufacturer: Bosch DS150i/DS160, or Securitron XMS.

2.05 POWER SUPPLY EQUIPMENT:

1. General: Power supplies shall be solid state and meet or exceed the manufacturer's recommendations for the individual devices served and meet the following minimum requirements:

a. Mounted in a NEMA 1 hinged enclosure with power indicator integral with door.

b. Rated at 1.2 times the current draw for devices served.

c. UL Class 2 rated and individually fused outputs to each device served.

2. Devices requiring common voltages shall be powered from a common power supply at the locations indicated on the Drawings.

3. Battery back-up

a. Batteries shall be sized to provide 105% capacity for the same time interval as the batteries in the security control console.

b. Standby batteries shall be sealed lead-calcium, lead-acid, or nickel-cadmium.

c. Controls shall be designed to maintain full battery charge when primary power is available. Batteries shall be recharged to 85% capacity within 24 hours from battery use.

d. Sufficient battery back-up to power devices connected for 30 min in the event of primary power failure.

e. Locking hardware power supplies shall have a UL Listed input for connection to a fire alarm panel output, which upon initiation shall disconnect power to the selected lock outputs. Coordinate with Division 8 for electrical power requirements.

4. Manufacturer: Alarm-Saf, Locknetics, or Securitron.

2.06 MISCELLANEOUS EQUIPMENT:

A. Fire/Life Safety Interface:

1. Locks shall be power, dual fail-safe type.

2. Locks shall be state fire marshal approved for perimeter locks, stair tower locks, and locks installed on required exit doors which empty into exit corridors, vestibules, stairwells, or building exits.

2.07 INTERCOM SYSTEMS:

A. General:

1. Provide SIP compliant IP compatible substations to be connected to the Owner's VOIP telephone system:

B. Substations:

1. Tamper resistant intercom station with the following features:

   a. Stainless steel front plate with recessed illuminated call button.

   b. A moisture resistant speaker and microphone shall be mounted behind 2 offset grills, milled into aluminum block to prevent damage from foreign material or water.

2. Audio:

   a. Audio quality:

      1) Speech transmission index (STI) - at 70 dB: > 0.8*

      2) Percentage articulation loss of consonants (Alcons) - at 70 dB : < 5%

      3) Total harmonic distortion + noise, without noise reduction (THD+N) - at 70 dB: < 2%.

   b. SPL rated power:

      1) At 1m in open duplex: 95 dB.

      2) At 1m in half duplex: 105 dB.

      3) At 1m in program distribution and announcement: 105 dB

   c. Noise cancelling features:

      1) Suppression of musical noise

      2) Suppression of static noise

      3) Suppression of rapidly changing noise

   d. Codecs: G.711, G.722

   e. Frequency range, G.722 Codec 200 Hz – 7000 Hz

f. Audio modes:

1) Full open duplex, switched open duplex

2) Adaptive jitter filter

3) Local tone generator

4) Audio mixing - 3 channels

5) Sound level detection (scream alarm)

6) Automatic gain control (microphone)

g. Internal speaker amplifier: 10 W class D

h. Microphone technology: Digital MEMS, omnidirectional microphone

3. Networking and protocols:

a. Protocols: IPv4 (with DiffServ), SIP, TCP, UDP, HTTPS, TFTP, RTP, DHCP, SNMP, STENTOFON CCoIP® , NTP

b. LAN protocols:

1) Power over Ethernet (IEEE 802.3 a-f)

2) VLAN(IEEE 802.1pq)

3) Network Access Control (IEEE 802.1x)

4) STP (IEEE 802.1d)

5) RSTP (IEEE 802.1d-2004)

c. Management and operation:

1) HTTP/HTTPS (Web configuration)

2) DHCP and static IP + STENTOFON Pulse™

3) Remote automatic software upgrade

4) Centralized monitoring

d. Advanced supervision functions shall include network test, tone test, status reports.

e. SIP support:

1) RFC 3261 (SIP base standard)

2) RFC 3215 (SIP refer)

3) RFC 2976 (SIP info)

f. DTMF support RFC 2833, 2976 (SIP info)

4. Environmental requirements and compliances:
a. IP rating: IP-66, tested according to EN 60529

b. IK rating IK 10, tested according to EN 62262

c. Operating temperature range: -13° to 158 ° F

d. Storage temperature range:-13° to 158 ° F

e. Relative humidity: < 95% not condensing

f. Corrosion: Salty mist, tested according to EN60945

g. Vibration Tested according to EN60945

h. UV-resistant

i. FCC Part 15

j. Compliances:

1) IEC/EN 50486 Equipment for use in audio video door-entry systems

5. Manufacturer: Stentofon Turbine or approved equal.

PART 3: EXECUTION

3.01 INTRUSION DETECTION SYSTEMS:

A. Programming:

1. Program zone configurations, names, and any other user-defined fields with terminology and descriptions provided by the Owner.

2. Program access rights, passcodes, ACAMS interface, holidays, area control, inputs and outputs, and schedules.

B. Alarm Monitoring Service:

1. Provide 1 year of alarm monitoring service with a UL listed central station. Include fees associated with connection, subscription, and termination so that no other costs shall be incurred if the service is terminated at the end of the year.

3.02 ACCESS CONTROL AND ALARM MONITORING SYSTEMS:

A. Configure field panel communications as indicated on the Drawings.

B. Access Control System Parameters:

1. Program the alarm bypass or shunt time (the time period the door can remain open before an alarm event is created) for 30 seconds, unless directed otherwise by the Owner's representative.

2. Program the door relock time (the time period after which the door will relock unless opened) for 5 seconds.

C. Programming:

1. Program alarm response fields, door names, and any other user-defined fields with terminology and descriptions provided by the Owner.

2. Program access rights, password protection, video surveillance system interface, holidays, area control, inputs and outputs, schedules, and elevator control.

D. Graphics:

1. Develop graphic maps that detail the facility and display inputs and outputs dynamically.

2. Utilize AutoCAD DWG architectural floor plans that show walls, doors, windows, room names, and room numbers.

E. System Integration and Interfaces:

1. The ACAMS shall interface with the video surveillance system to cause automatic camera call-up as follows:

   a. Upon an alarm condition at but not limited to, an access point, duress button or other alarm input, the ACAMS shall cause the video surveillance system to automatically call up the associated video camera image on the designated video surveillance monitor or multi-display monitor segment.

   b. Additionally the alarm condition shall also be able to automatically cause the video image to be displayed in a window on the ACAMS operator workstation on demand. This shall apply to both thin client (web-client) workstations and workstation with ACAMS client software loaded.

   c. The system shall be programmed with at least one video camera call-up for each access control and alarm point.

F. Programming Requirements and Deliverables:

1. Produce questionnaires to solicit user input for programming the system. The questionnaires shall identify each programming item that requires user input to configure the ACAMS along with recommendations for responses. These questionnaires shall be finalized in a series of meetings with the Owner's designated agent until such time that the questionnaires are completed and the Owner has authorized the information to be inputted into the ACAMS.

2. The questionnaires shall include three series.

   a. The first shall be devoted to alarm input and door hardware programming, or hardware related programming.

   b. The second shall be devoted to interface programming and associated action and reaction requirements including the video surveillance system call-up and switching requirements.

   c. The third shall be related to display of alarm messaging, mapping and any requirements for alarm responses and reporting.

3. Upon completion, the programming questionnaires and associated programming database sheets shall be included in the O&M manuals.

G. The following minimum requirements shall be addressed during the programming:

1. Each door prop and or door forced open alarm event shall result in the following actions:

   a. The video signal for the associated video camera shall be switched to the first available event monitor of the associated workstation or console.

   b. Where pan-tilt-zoom cameras are associated with the alarm, the camera shall be panned and tilted, and the lens zoomed to provide an acceptable (Owner approved) view of the alarm scene.

   c. Where pan-tilt-zoom video cameras are associated with the alarm, the video camera shall be automatically selected for local control via the video surveillance system command keyboard.

   d. The video signal for the associated video camera shall be recorded on the video surveillance system network recorder at a frame rate of min. 15 frames per second and at the highest resolution the associated camera offers for the duration of the event. The video clip shall also be tagged to be associated with the ACAMS alarm condition identification for future retrieval during ACAMS journal replay.

   e. A supervised and coded alarm signal shall be transmitted to the associated workstations or consoles causing an audible and visual alarm signal.

   f. Where a local door sounder is located adjacent to the door, the sounder alarm shall be activated until reset at the workstation or console.

   g. A graphical representation of the alarm scene (site or floor plan) with icons representing the open door, video camera, and other local devices shall be displayed on the graphical user interface (GUI). Icons representing active devices shall change color to indicate their state change (inactive to active).

2. Each duress alarm event shall result in the following actions:

   a. The video signal for the associated video camera shall be switched to the first available event monitor of the associated workstation or console.

b. Where pan-tilt-zoom video cameras are associated with the alarm, the camera shall be panned and tilted, and the lens zoomed to provide an acceptable (Owner approved) view of the alarm scene.

c. Where pan-tilt-zoom video cameras are associated with the alarm, the video camera shall be automatically selected for local control via the video surveillance system command keyboard.

d. The video signal for the associated video camera shall be recorded on the video surveillance system network recorder at a frame rate of min. 15 frames per second and at the highest resolution the associated camera offers for the duration of the event. The video clip shall also be tagged to be associated with the ACAMS alarm condition identification for future retrieval during ACAMS journal replay.

e. A supervised and coded alarm signal shall be transmitted to the associated workstations or consoles causing an audible and visual alarm signal.

f. A graphical representation of the alarm scene (site or floor plan) with icons representing the duress pushbutton, video camera, and other local devices shall be displayed on the graphical user interface. Icons representing active devices shall change color to indicate their state change (inactive to active).

3. Each authorized door access event shall result in the following actions:

a. The video signal for the associated video camera shall be switched to the first available event monitor of the associated workstation or console.

b. Where pan-tilt-zoom video cameras are associated with the alarm, the camera shall be panned and tilted, and the lens zoomed to provide an acceptable (Owner approved) view of the access scene.

c. Where pan-tilt-zoom video cameras are associated with the alarm, the video camera shall be automatically selected for local control via the video surveillance system command keyboard.

d. The video signal for the associated video camera shall be recorded on the video surveillance system network recorder at a frame rate of min. 15 frames per second and at the highest resolution the associated camera offers for the duration of the event. The video clip shall also be tagged to be associated with the ACAMS alarm condition identification for future retrieval during ACAMS journal replay.

e. A supervised and coded access signal shall be transmitted to the associated workstations or consoles.

4. Each unauthorized door access event shall result in the following actions:

a. The video signal for the associated video camera shall be switched to the first available event monitor of the associated workstation or console.

b. Where pan-tilt-zoom video cameras are associated with the alarm, the camera shall be panned and tilted, and the lens zoomed to provide an acceptable (Owner approved) view of the alarm scene.

c. Where pan-tilt-zoom video cameras are associated with the alarm, the video camera shall be automatically selected for local control via the video surveillance system command keyboard.

d. The video signal for the associated video camera shall be recorded on the video surveillance system network recorder at a frame rate of min. 15 frames per second and at the highest resolution the associated camera offers for the duration of the event. The video clip shall also be tagged to be associated with the ACAMS alarm condition identification for future retrieval during ACAMS journal replay.

e. A supervised and coded alarm signal shall be transmitted to the associated workstations or consoles causing an audible and visual alarm signal.

f. A graphical representation of the alarm scene (site or floor plan) with icons representing the devices shall be displayed on the graphical user interface. Icons representing active devices shall change color to indicate their state change (inactive to active).

5. Each video motion detection alarm shall result in the following actions:

a. The video signal for the associated video camera shall be switched to the first available event monitor of the associated workstation or console.

b. Where pan-tilt-zoom video cameras are associated with the alarm, the camera shall be panned and tilted, and the lens zoomed to provide an acceptable (Owner approved) view of the alarm scene.

c. Where pan-tilt-zoom video cameras are associated with the alarm, the video camera shall be automatically selected for local control via the video surveillance system command keyboard.

d. The video signal for the associated video camera shall be recorded on the video surveillance system network recorder at a frame rate of min. 15 frames per second and at the highest resolution the associated camera offers for the duration of the event. The video clip shall also be tagged to be associated with the ACAMS alarm condition identification for future retrieval during ACAMS journal replay.

e. A supervised and coded alarm signal shall be transmitted to the associated workstations or consoles causing an audible and visual alarm signal.

f. A graphical representation of the alarm scene (site or floor plan) with icons representing the camera and other local devices shall be displayed on the graphical user interface. Icons representing active devices shall change color to indicate their state change (inactive to active).

H. Cardholder Enrollment:

1. Provide fill-in-the-blank forms to the Owner requesting needed information.

3.03 INTERCOM SYSTEMS:

A. Connect intercom substations to the Owner's VoIP telephone system and coordinate programming requirements.

3.04 KEYS:

A. Permanently identify with metal tags.

B. Turn over keys, along with manufacturer's certificate stating the quantity of each key made, to the Owner and obtain a signed receipt acknowledging receipt of same.

3.05 MISCELLANEOUS EQUIPMENT:

A. Fire/Life Safety Interface:

1. Any device installed to lock or unlock emergency exits shall be connected to the building fire alarm system to unlock the door in the direction of egress in a fire alarm condition, or on loss of power to the fire alarm control panel.

2. Emergency exits locked in the direction of egress shall unlock on loss of primary power to the building. The use of battery or emergency power shall not be used to keep emergency exits locked in the path of egress.

3.06 POWER SUPPLY EQUIPMENT:

A. Components specified below shall be provided with battery back-up or connected to the UPS:

1. Detection devices.

2. ACAM controllers, Card access readers, reader interface devices, request to exit motion detectors.

3. IDS control panels.

B. Components specified below shall be connected in their respective locations to the UPS:

1. ACAMS servers and associated monitors.

2. ACAMS workstations and associated monitors.

3. Security devices located in the telecommunications rooms equipment racks.

3.07 CABLES:

A. Size power conductors as required to ensure voltage drop does not exceed 10% of the source voltage of the load.

B. Data cables shall be as recommended by the manufacturer.

END OF SECTION 28 10 00

SECTION 28 11 00
VIDEO SURVEILLANCE SYSTEMS

PART 1: GENERAL

1.01 DESCRIPTION:

A. This Section covers video surveillance systems.

B. Video surveillance systems general provisions are specified in Section 28 00 10, Security General.

C. Video surveillance systems performance verification is specified in Section 28 00 90, Security Performance Verification.

1.02 QUALITY ASSURANCE:

A. Installation of the video surveillance system (VSS) shall be under the direct on-site supervision of a person or persons having completed the manufacturer's highest available certification program, and have direct field experience in the installation of a minimum three project of similar scope and size within the past 5 years. In addition the installation company shall have at the minimum two permanently employed persons with current system certification in their field office directly responsible for the installation and ongoing maintenance of the project. The office shall be located within 100 mile radius of the project.

B. All field technicians shall have completed as a minimum, the factory training recommended by the manufacturer of the system provided.

C. The installation company shall be a currently listed as an authorized dealer or business partner by the manufacturer of the system provided, and shall have been listed as such for a minimum of 3 years.

PART 2: PRODUCTS

2.01 GENERAL:

A. Unless otherwise specified herein, quantities of equipment are indicated on the Drawings.

B. The video surveillance system shall consist of IP (TCIP compatible) video cameras viewable on video surveillance workstations via a local area network. The video signals from the cameras shall be recorded on the network video recorders and server-recorders.

C. Provide compatible components. Provide IP cameras that are compatible with the network video recorders video management system software provided. Provide pan-tilt drives that are compatible with the pan-tilt drive control systems video surveillance management system software provided. Provide network video recorders video surveillance management system software compatible with the access control and alarm monitoring system software provided under Section 28 10 00, Security Systems.

2.02 VIDEO CAMERAS AND ACCESSORIES:

A. Video cameras shall have the following minimum features:

1. Signal and scanning systems: NTSC color.

2. Resolution: As indicated in the Drawings.

3. Video surveillance cameras shall be IP compatible with the following minimum features:

a. Network interface: Ethernet 10/100Base-T.

b. Supported protocols: TCP/IP, UDP/IP, DHCP, HTTP, Multicast, PPPoE, RTP, and RTSP.

c. Security: SSL-based authentication.

d. Compression: dual-stream MPEG4 or H.264, each stream independently selectable and capable of being transmitted to separate locations.

e. Frame rates: 2 frames per second, 4 frames per second, 10 frames per second, 15 frames per second, and 30 frames per second, selectable.

f. Resolution: 4CIF or D1, 2CIF, and CIF, scalable. Video cameras designated as megapixel video cameras shall be provide HD, D1, 2CIF, and CIF, scalable.

4. Progressive scan or virtual progressive scan CCD.

5. IP cameras shall be POE (12V DC, 12 W maximum). Provide 12 or 24VAC or DC operation with phase-adjustable line-lock for use on mixed AC power phases for outdoor cameras where heater or blower is required.

6. Manufacturer: Axis, Avigilon, Bosch, Panasonic, Pelco, Samsung, Sony, or Toshiba

B. Camera lenses shall have the following minimum features:

1. For fixed position cameras:

a. Variable focal length lenses designed for the field of view indicated on the Drawings to be covered.

b. Auto iris.

c. Compatible with the camera provided.

2. For remotely positionable (PTZ) cameras:

a. A 23X or higher optical zoom lens.

b. Auto iris.

c. Compatible with the camera provided.

C. Pan-tilt drives (for remotely positionable cameras) shall have the following minimum features:

1. Pan movement: 360° continuous pan rotation.

2. Vertical tilt: unobstructed 85°.

3. Manual pan-tilt speed: 100° per second.

4. Preset pan-tilt speed: 200° per second.

5. Capable of 64 presets.

6. Auto-flip feature that rotates the camera 180° at the bottom of tilt travel.

D. Pan-Tilt-Zoom Control Receivers:

1. Receivers shall be compatible with the switching and control system provided herein.

2. For receivers located in environmentally controlled areas (indoors), provide a NEMA 1 enclosure. For receivers located in environmentally uncontrolled areas (outdoors), provide a NEMA 4 enclosure.

3. Manufacturer: provide high speed dome camera units manufactured by the same company that manufactures the switching and control system provided herein: Axis, Bosch, Panasonic, or Pelco.

E. Camera Enclosures and Mounting Hardware:

1. For cameras located in environmentally controlled areas (indoors) enclosures and mounting hardware shall have the following minimum features:

a. Compatible with the camera and lens provided.

b. NEMA 1 or NEMA 4 enclosure.

c. Enclosures and mounting hardware of the style and type indicated on the Drawings.

2. For each cameras located in environmentally uncontrolled areas (outdoors) enclosures and appropriate mounting hardware shall have the following minimum features:

a. Compatible with the camera, lens, and pan-tilt drive provided.

b. NEMA 4 enclosure.

c. Integral heater where cameras exposed to wind and ice are not rated for -22° F or lower.

d. Sunshield where the video camera is exposed to direct sun.

e. Integral blower.

f. Enclosures and mounting hardware of the style and type indicated on the Drawings.

2.03 NETWORK-BASED VIDEO SURVEILLANCE SYSTEMS:

A. General:

1. The video surveillance system shall receive video signals over a local area network or wide area network from IP video cameras directly connected to the network, and analog cameras connected to the network via video network encoders.

B. Video Server-Recorders:

1. Processors: Intel Xeon Quad Core 2.33 GHz CPUs.

2. Memory: 8 GB of SDRAM.

3. Controllers: SCSI-3 or SATA II RAID-5.

4. Provide sufficient hard drive storage capacity (internal or external) to store or archive the images from each video camera for the required length of time, and at the resolution, quality and frame rate as indicated on the drawings.

5. Hard drives shall be hot swappable in a RAID-5 configuration, min 10,000RPM.

6. Optical drives: DVD-R/W.

7. Dual network cards: 10/100/1000Base-T.

8. Monitors: 17" color LCD with integrated KVM and slide-away rack mount kit as specified herein.

9. Redundant power supplies.

10. Automatic data aging to allow the automatic deletion of non-even related or non-alarm video frames based on user setting of time interval.

11. Other components required for a complete and operational system.

12. Operating system: Linux, Windows Server 2003 R2, or Windows Server 2008.

13. These are minimum requirements. Provide servers that meet the video management software manufacturer’s recommendations, where the system manufacturer’s recommendations exceed these requirements.

14. Manufacturers: Avigilon, DNF Storage Falcon series, Exacq Technologies 4U Rackmount IP Servers, Pelco Endura NSM series, NICE, Dell or HP.

C. Video Workstations (Clients):

1. Processors: Intel Quad Core Xeon 3.6 GHz CPU.

2. RAM: 16 GB of SDRAM.

3. Internal storage: 1 TB SATA II hard drive.

4. Optical drives: DVD-R/W.

5. Network cards: 10/100/1000Base-T.

6. Video card with min 1GB NVRAM and dual HDMI or display port monitor output.

7. Min 20" color LCD monitors with a minimum resolution: 1600 x 1280 pixels. Provide quantity and exact size as indicated on the drawings.

8. Other components required for a complete and operational system, including optical mouse and keyboard.

9. Operating system: Windows 7 Professional, or Windows 8 Professional.

10. These are minimum requirements. Provide workstations that meet the video management software manufacturer's recommendations, where the system manufacturer's recommendations exceed these requirements.

D. Video Surveillance Management System Applications Software:

1. General: provide network video management software specifically designed for video surveillance applications with the following minimum features:

   a. Compatible with video cameras and servers specified herein.

   b. Compatible at a software level with the access control systems specified in Section 28 10 00, Security Systems to allow automatic events such as video call-up based on access control events, and automatic software tagging of video clips to enable retrieval of event related video from the access control system operator interface.

   c. Compatible with MJPEG, MPEG2, MPEG4, and H.264 compression algorithms.

   d. Capable to store video on two separate servers (at two separate locations). Provide open architecture software.

2. The application software shall support the following minimum capabilities:

a. Live viewing and recording unlimited number of cameras on multiple servers at multiple locations. Support for any number of cameras with increments of 1 camera. , up to 64 cameras per server.

b. Simultaneous recording and viewing of MJPEG, MPEG2, MPEG4, and H.264 compression formats.

c. Manual and preset control of pan and tilt functions of camera pan-tilt drive mechanisms, and zoom-control of camera lenses.

d. Recording of camera inputs and activation of camera outputs.

e. Alerting via e-mail and SMS-texting.

f. Restricting access via password protection.

g. Web access via browser-based client.

h. Data-aging capability to allow automatic deletion of non-event related video frames based on user settings after a user pre-set amount of days.

i. Active directory support.

j. Multisite, multi-server access.

k. Video/audio export formats including JPEG (still images), AVI, and WAV.

l. Manufacturer: Avigilon, Exacq, Milestone, NICE, ONSSI Ocularis or Pelco Endura.

2.04 VIDEO MONITORS:

A. 24" (diagonal) widescreen flat panel monitors with the following minimum features:

1. Imaging technology: LCD, 16:9 aspect ratio, NTSC.

2. Brightness: 300 cd/m^2.

3. Native resolution: 1920 x 1200.

4. Maximum resolution: 1920 x 1200.

5. Screen size: 20" viewable.

6. Contrast ratio: 800:1.

7. Response time: 5 ms (gray to gray).

8. Pixel pitch: 0.258".

9. Compatibility: PC and MAC.

10. Computer/video input support: HDMI or DVI-D (24-pin digital DVI).

11. Power requirements: 100 V to 240 V AC, Energy Star 4.0 compliant.

12. Manufacturer: Dell, Mitsubishi, NEC, Samsung, Sharp, Sony, or Viewsonic.

B. Rack mountable 17" (diagonal) flat panel monitors with integral KVM switch and keyboard in sliding housing designed for mounting in a 19" EIA rack with the following minimum features:

1. Mounted in 1 RU sliding housing.

2. Imaging technology: LCD, 4:3 aspect ratio, NTSC.

3. Native resolution: 1280 x 1024.

4. Maximum resolution: 1280 x 1024.

5. Screen size: 17" viewable.

6. DDC emulation of the monitor.

7. Integral keyboard.

8. KVM ports: 1 SPHD-15 female.

9. Dual interface support: PS/2 or USB keyboard and mouse data transfer from the switch to the computer.

10. Multiplatform support: Windows 7 or higher, Mac 8.6 or higher, Linux Red Hat 7.1 or higher, and Sun Solaris.

11. Computer ports: 8 HDB-15 female.

12. Power requirements: 100 V to 240 V AC.

13. Manufacturer: ATEN CL-1758 Slideaway LCD KVM Switch or approved equal.

2.05 MISCELLANEOUS EQUIPMENT:

A. Power supplies: 24VAC, sized to accommodate video cameras and devices indicated on the Drawings with a 25% margin for future expansion, and shall have the following features:

1. Compliance with UL 2044-2008.

2. 120 V AC input.

3. One individually fused output per camera.

4. Standard 19" rack mounted enclosure.

5. Manufacturer: Altronix or approved equal.

PART 3: EXECUTION

3.01 GENERAL:

A. Provide programming for complete systems integration with the access control and alarm monitoring systems and the intercom systems as specified herein and in Section 28 10 00, Security Systems.

B. Systems shall be installed by skilled craftsmen in a manner conforming to industry standards for the craft.

3.02 PROGRAMMING REQUIREMENTS AND DELIVERABLES:

1. Produce questionnaires to solicit user input for programming the system. The questionnaires shall identify each programming item that requires user input to configure the VSS along with recommendations for responses. These questionnaires shall be finalized in a series of meetings with the Owner's designated agent until such time that the questionnaires are completed and the Owner has authorized the information to be entered into the VSS.

2. The questionnaires shall include three series.

a. The first shall be devoted to network configuration, IP addressing, VLAN and other network related programming.

b. The second shall be devoted to camera naming conventions and associated action and reaction requirements including the video surveillance system call-up and switching requirements.

c. The third shall be related to the VSS server and workstation configuration, including user configuration, recording parameters for cameras, storage management, web access and operator environment configuration.

3. Upon completion, the programming questionnaires and associated programming database sheets shall be included in the O&M manuals.

B. Video cameras: Program all configurable parameters as required for the specified system operation.

C. Pan-tilt drives: program presets as required for coverage of the detection devices, sensors, and alarm zones indicated on the Drawings.

1. Network-Based Video Surveillance Systems: Configure the network addresses, security settings, recording settings, camera naming, and other parameters per the Owner's requirements as appropriate and in accordance to meet equipment manufacturer’s requirements.

3.03 VIDEO MONITORS:

A. Provide support structure where needed to support wall-mounted flat panel monitors.

B. Configure monitor settings as appropriate for the operation of the system as configured.

END OF SECTION 28 11 00