- Arc flash incident energy at the working distance (calories/ cm^2)
- PPE category and description including the glove rating
- Voltage rating of the equipment
- Limited approach distance (inches)
- Restricted approach distance (inches)
- Prohibited approach distance (inches)
- Equipment/bus name
- Date prepared
- Consultant name and address

F. Equipment Verification/Operation: The validity of the arc flash study and incident energy readings is in part based on proper setting of overcurrent device trip times and the proper operation of the overcurrent devices and breakers themselves. The consultant shall verify proper operation of overcurrent devices and breakers at the request using InterNational Electrical Testing Association (NETA) qualified technicians.

The consultant shall be capable of adjustment, maintenance, repair or replacement of overcurrent devices or breakers as required to support the performance of the electrical system in line with the expectations of the system study.

G. Safety Training: The consultant shall provide XYZ Company one day of arc flash safety training that contains the requirements referenced in OSHA 1910.269, OSHA 1910 Subpart S and NFPA 70E. This shall include:

- Proper use of the system analysis data
- Interpretation of hazard labels
- Selection and utilization of personal protective equipment
- Safe work practices and procedures

H. The consultant shall provide an outline of the one-day training course including training materials. The consultant shall be capable of developing and presenting customized training for approval as required. The consultant shall provide a training certificate to record satisfactory completion by XYZ Company employees for continuing education credits and re-licensing requirements. Satisfactory completion is defined as the student obtaining a minimum of 70% on the post training examination and the ability to work safely if a hands on performance evaluation is provided

H. Safety Documentation/Policy: The consultant shall integrate the results of the system study and design review into the safety manual in compliance with OSHA CFR 29 1910.333. The consultant shall assist at its request to develop a safety policy with corresponding documentation and procedures including information gained in the system analysis. This includes electrical safety, procedures for mitigation of arc hazards, PPE selection based on specific equipment, task and training requirements.

1.01 QUALITY ASSURANCE

A. The consultant shall provide all necessary material, equipment, labor, and technical supervision to perform the arc flash hazard analysis as described herein.

B. The consultant shall utilize engineers and technicians that are experienced and regularly perform electrical power system testing.

C. Personnel performing the arc flash analysis shall be trained and experienced in accordance with NETA Training Specifications concerning the apparatus and systems being

evaluated. These individuals shall be capable of conducting the tasks of the analysis in a safe manner and with complete knowledge of the hazards involved.

1.04 SAFETY AND PROCEDURAL REQUIREMENTS

A. The consultant must provide proof (written documentation) that its employees have been properly trained in the use and application of personal protective equipment (PPE) and the hazards of working on or near energized equipment. The consultant must provide its own PPE protection with a minimum arc thermal performance rating (ATPV) of 40 calories/cm^2.

B. Safety practices that shall be followed include, but are not limited to, the following:

- Occupational Safety and Health Act
- *Accident Prevention Manual for Industrial Operations*, National Safety Council
- Applicable state and local safety operating procedures
- Owner's safety practices

C. Perform all work in accordance with the applicable codes and standards of the following agencies except as provided otherwise herein:

1. InterNational Electrical Testing Association – NETA ATS latest Edition: Acceptance Testing Specifications, and/or NETA MTS latest Edition: Maintenance Testing Specifications.
2. National Fire Protection Association – NFPA
    a. ANSI/NFPA 70: National Electrical Code
    b. ANSI/NFPA 70B: Recommended Practice for Electrical Equipment Maintenance
    c. NFPA 70E: Electrical Safety Requirements for Employee Workplaces

***** END OF SECTION *****

SECTION 26 24 16

PANELBOARDS

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. Section Includes:

1. Lighting and appliance branch-circuit panelboards.

1.3 SUBMITTALS

A. Product Data: For each type of panelboard, switching and overcurrent protective device, transient voltage suppression device, accessory, and component indicated. Include dimensions and manufacturers' technical data on features, performance, electrical characteristics, ratings, and finishes.

B. Shop Drawings: For each panelboard and related equipment.

1. Include dimensioned plans, elevations, sections, and details. Show tabulations of installed devices, equipment features, and ratings.

2. Detail enclosure types and details for types other than NEMA 250, Type 1.

3. Detail bus configuration, current, and voltage ratings.

4. Short-circuit current rating of panelboards and overcurrent protective devices.

5. Include evidence of NRTL listing for series rating of installed devices.

6. Detail features, characteristics, ratings, and factory settings of individual overcurrent protective devices and auxiliary components.

7. Include wiring diagrams for power, signal, and control wiring.

8. Include time-current coordination curves for each type and rating of overcurrent protective device included in panelboards. Submit on translucent log-log graft paper; include selectable ranges for each type of overcurrent protective device.

C. Field Quality-Control Reports:

1. Test procedures used.

2. Test results that comply with requirements.

3. Results of failed tests and corrective action taken to achieve test results that comply with requirements.

D. Panelboard Schedules: Typed schedule for installation in panelboards.

E. Operation and Maintenance Data: For panelboards and components to include in emergency, operation, and maintenance manuals. In addition to items specified in Division 01 Section "Operation and Maintenance Data," include the following:

1. Manufacturer's written instructions for testing and adjusting overcurrent protective devices.

2. Time-current curves, including selectable ranges for each type of overcurrent protective device that allows adjustments.

1.4 QUALITY ASSURANCE

A. Source Limitations: Obtain panelboards, overcurrent protective devices, components, and accessories from single source from single manufacturer.

B. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

C. Comply with NEMA PB 1.

D. Comply with NFPA 70.

1.5 DELIVERY, STORAGE, AND HANDLING

A. Remove loose packing and flammable materials from inside panelboards; install temporary electric heating (250 W per panelboard) to prevent condensation.

B. Handle and prepare panelboards for installation according to NECA 407 and NEMA PB 1.

1.6 WARRANTY

A. Special Warranty: Manufacturer's standard form in which manufacturer agrees to repair or replace transient voltage suppression devices that fail in materials or workmanship within specified warranty period.

1. Warranty Period: [Five] <Insert number> years from date of Substantial Completion.

PART 2 - PRODUCTS

2.1 GENERAL REQUIREMENTS FOR PANELBOARDS

A. Enclosures: Flush-mounted cabinets.

1. Rated for environmental conditions at installed location.

a. Indoor Dry and Clean Locations: NEMA 250, Type 1.

2. Front: Secured to box with concealed trim clamps. For surface-mounted fronts, match box dimensions; for flush-mounted fronts, overlap box.

3. Hinged Front Cover: Entire front trim hinged to box and with standard door within hinged trim cover.

4. Finishes:

a. Panels and Trim: Steel and galvanized steel, factory finished immediately after cleaning and pretreating with manufacturer's standard two-coat, baked-on finish consisting of prime coat and thermosetting topcoat.

b. Back Boxes: Same finish as panels and trim.

5. Directory Card: Inside panelboard door, mounted in metal frame with transparent protective cover.

B. Phase, Neutral, and Ground Buses:

1. Material: Hard-drawn copper, 98 percent conductivity.

2. Equipment Ground Bus: Adequate for feeder and branch-circuit equipment grounding conductors; bonded to box.

C. Conductor Connectors: Suitable for use with conductor material and sizes.

1. Material: Hard-drawn copper, 98 percent conductivity.

2. Main and Neutral Lugs: Compression or Mechanical type.

3. Ground Lugs and Bus-Configured Terminators: Compression or Mechanical type.

D. Future Devices: Mounting brackets, bus connections, filler plates, and necessary appurtenances required for future installation of devices.

E. Panelboard Short-Circuit Current Rating: Fully rated to interrupt symmetrical short-circuit current available at terminals.

2.2 LIGHTING AND APPLIANCE BRANCH-CIRCUIT PANELBOARDS

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

1. Square D; a brand of Schneider Electric.

B. Panelboards: NEMA PB 1, lighting and appliance branch-circuit type.

C. Mains: Circuit breaker or lugs only.

D. Branch Overcurrent Protective Devices: Bolt-on circuit breakers, replaceable without disturbing adjacent units.

E. Doors: Concealed hinges; secured with flush latch with tumbler lock; keyed alike.

2.3 OVERCURRENT PROTECTIVE DEVICES

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

1. Square D; a brand of Schneider Electric.

B. Molded-Case Circuit Breaker (MCCB): Comply with UL 489, with interrupting capacity to meet available fault currents.

1. Thermal-Magnetic Circuit Breakers: Inverse time-current element for low-level overloads, and instantaneous magnetic trip element for short circuits. Adjustable magnetic trip setting for circuit-breaker frame sizes 250 A and larger.

2. Adjustable Instantaneous-Trip Circuit Breakers: Magnetic trip element with front-mounted, field-adjustable trip setting.

3. Molded-Case Circuit-Breaker (MCCB) Features and Accessories:

a. Standard frame sizes, trip ratings, and number of poles.

b. Lugs: Compression or Mechanical style, suitable for number, size, trip ratings, and conductor materials.

c. Multipole units enclosed in a single housing or factory assembled to operate as a single unit.

d. Handle Padlocking Device: Fixed attachment, for locking circuit-breaker handle in on or off position.

e. Handle Clamp: Loose attachment, for holding circuit-breaker handle in on position.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Receive, inspect, handle, and store panelboards according to NECA 407 and NEMA PB 1.1.

B. Examine panelboards before installation. Reject panelboards that are damaged or rusted or have been subjected to water saturation.

C. Examine elements and surfaces to receive panelboards for compliance with installation tolerances and other conditions affecting performance of the Work.

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

3.2 INSTALLATION

A. Install panelboards and accessories according to NECA 407 and NEMA PB 1.1.

B. Mount top of trim 90 inches (2286 mm) above finished floor unless otherwise indicated.

C. Mount panelboard cabinet plumb and rigid without distortion of box. Mount recessed panelboards with fronts uniformly flush with wall finish and mating with back box.

D. Install overcurrent protective devices and controllers not already factory installed.

1. Set field-adjustable, circuit-breaker trip ranges.

E. Install filler plates in unused spaces.

F. Stub six 1-inch (27-GRC) empty conduits from panelboard into ceiling space.

G. Arrange conductors in gutters into groups and bundle and wrap with wire ties.

H. Comply with NECA 1.

3.3 IDENTIFICATION

A. Identify field-installed conductors, interconnecting wiring, and components; provide warning signs complying with Division 26 Section "Identification for Electrical Systems."

B. Create a directory to indicate installed circuit loads; incorporate Owner's final room designations. Obtain approval before installing. Use a computer or typewriter to create directory; handwritten directories are not acceptable.

C. Panelboard Nameplates: Label each panelboard with a nameplate complying with requirements for identification specified in Division 26 Section "Identification for Electrical Systems."

3.4 FIELD QUALITY CONTROL

A. Testing: Perform tests and inspections.

B. Acceptance Testing:

1. Test insulation resistance for each panelboard bus, component, connecting supply, feeder, and control circuit.

2. Test continuity of each circuit.

C. Tests and Inspections:

1. Perform each visual and mechanical inspection and electrical test stated in NETA Acceptance Testing Specification. Certify compliance with test parameters.

2. Correct malfunctioning units on-site, where possible, and retest to demonstrate compliance; otherwise, replace with new units and retest.

3. Perform the following infrared scan tests and inspections and prepare reports:

a. Initial Infrared Scanning: Perform an infrared scan of each panelboard. Remove front panels so joints and connections are accessible to portable scanner.

b. Instruments and Equipment:

1) Use an infrared scanning device designed to measure temperature or to detect significant deviations from normal values. Provide calibration record for device.

D. Panelboards will be considered defective if they do not pass tests and inspections.

E. Prepare test and inspection reports, including a report that identifies panelboards included and that describes scanning results. Include notation of deficiencies detected, remedial action taken, and observations after remedial action.

3.5 ADJUSTING

A. Adjust moving parts and operable component to function smoothly, and lubricate as recommended by manufacturer.

B. Set field-adjustable circuit-breaker trip ranges as indicated as specified in Division 26 Section "Overcurrent Protective Device Coordination Study."

END OF SECTION

THIS PAGE IS INTENTIONALLY BLANK

SECTION 26 28 13

FUSES

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. Section Includes:

1. Cartridge fuses rated 600-V ac and less for use in enclosed switches.

B. Product Data: For each type of product indicated. Include construction details, material, dimensions, descriptions of individual components for each fuse type indicated:

1. Dimensions and manufacturer's technical data on features, performance, electrical characteristics, and ratings.

2. Current-limitation curves for fuses with current-limiting characteristics.

3. Time-current coordination curves (average melt) and current-limitation curves (instantaneous peak let-through current) for each type and rating of fuse.

4. Coordination charts and tables and related data.

1.3 QUALITY ASSURANCE

A. Source Limitations: Obtain fuses, for use within a specific product or circuit, from single source from single manufacturer.

B. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

C. Comply with NEMA FU 1 for cartridge fuses.

D. Comply with NFPA 70.

1.4 COORDINATION

A. Coordinate fuse ratings with utilization equipment nameplate limitations of maximum fuse size and with system short-circuit current levels.

1.5 EXTRA MATERIALS

A. Furnish extra materials that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.

1. Fuses: Nine of each size and type.

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. Cooper Bussmann, Inc.

2. Edison Fuse, Inc.

3. Ferraz Shawmut, Inc.

4. Littelfuse, Inc.

2.2 CARTRIDGE FUSES

A. Characteristics: NEMA FU 1, nonrenewable cartridge fuses with voltage ratings consistent with circuit voltages.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Examine fuses before installation. Reject fuses that are moisture damaged or physically damaged.

B. Examine holders to receive fuses for compliance with installation tolerances and other conditions affecting performance, such as rejection features.

C. Examine utilization equipment nameplates and installation instructions. Install fuses of sizes and with characteristics appropriate for each piece of equipment.

D. Evaluate ambient temperatures to determine if fuse rating adjustment factors must be applied to fuse ratings.

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

3.2 INSTALLATION

A. Install fuses in fusible devices. Arrange fuses so rating information is readable without removing fuse.

3.3 IDENTIFICATION

A. Install labels complying with requirements for identification specified in Division 26 Section "Identification for Electrical Systems" and indicating fuse replacement information on inside door of each fused switch and adjacent to each fuse block, socket, and holder.

***** END OF SECTION *****

SECTION 26 28 16

ENCLOSED SWITCHES AND CIRCUIT BREAKERS

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and other Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. Section Includes:

1. Fusible switches.
2. Nonfusible switches.
3. Enclosures.

1.3 DEFINITIONS

A. NC: Normally closed.

B. NO: Normally open.

C. SPDT: Single pole, double throw.

1.4 SUBMITTALS

A. Product Data: For each type of enclosed switch, circuit breaker, accessory, and component indicated. Include dimensioned elevations, sections, weights, and manufacturers' technical data on features, performance, electrical characteristics, ratings, accessories, and finishes.

1. Enclosure types and details for types other than NEMA 250, Type 1.
2. Current and voltage ratings.
3. Short-circuit current ratings (interrupting and withstand, as appropriate).
4. Include evidence of NRTL listing for series rating of installed devices.
5. Detail features, characteristics, ratings, and factory settings of individual overcurrent protective devices, accessories, and auxiliary components.
6. Include time-current coordination curves (average melt) for each type and rating of overcurrent protective device; include selectable ranges for each type of overcurrent protective device.
7. OSHPD OSP data sheet.

B. Operation and Maintenance Data: For enclosed switches and circuit breakers to include in emergency, operation, and maintenance manuals. In addition to items specified in Division 01 Section "Operation and Maintenance Data," include the following:

1. Manufacturer's written instructions for testing and adjusting enclosed switches and circuit breakers.
2. Time-current coordination curves (average melt) for each type and rating of overcurrent protective device; include selectable ranges for each type of overcurrent protective device.

1.5 QUALITY ASSURANCE

A. Source Limitations: Obtain enclosed switches and circuit breakers, overcurrent protective devices, components, and accessories, within same product category, from single source from single manufacturer.

B. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

C. Comply with NFPA 70.

1.6 COORDINATION

A. Coordinate layout and installation of switches, circuit breakers, and components with equipment served and adjacent surfaces. Maintain required workspace clearances and required clearances for equipment access doors and panels.

1.7 EXTRA MATERIALS

A. Furnish extra materials that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.

1. Fuses: Nine of each size and type.

2. Fuse Pullers: Two for each size and type.

PART 2 - PRODUCTS

2.1 FUSIBLE SWITCHES

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

1. Square D; a brand of Schneider Electric.

B. Type HD, Heavy Duty, Single Throw, 600-V ac, 1200 A and Smaller: UL 98 and NEMA KS 1, horsepower rated, with clips or bolt pads to accommodate specified fuses, lockable handle with capability to accept three padlocks, and interlocked with cover in closed position.

C. Accessories:

1. Equipment Ground Kit: Internally mounted and labeled for copper ground conductors.

2. Neutral Kit: Internally mounted; insulated, capable of being grounded and bonded; labeled for copper neutral conductors.

3. Lugs: Mechanical or Compression type, suitable for number, size, and conductor material.

2.2 NONFUSIBLE SWITCHES

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

1. Square D; a brand of Schneider Electric.

B. Type HD, Heavy Duty, Single Throw, 600-V ac, 1200 A and Smaller: UL 98 and NEMA KS 1, horsepower rated, lockable handle with capability to accept three padlocks, and interlocked with cover in closed position.

C. Accessories:

1. Equipment Ground Kit: Internally mounted and labeled for copper ground conductors.

2. Neutral Kit: Internally mounted; insulated, capable of being grounded and bonded; labeled for copper neutral conductors.

3. Lugs: Mechanical or Compression type, suitable for number, size, and conductor material.

2.3 ENCLOSURES

A. Enclosed Switches: NEMA AB 1, NEMA KS 1, NEMA 250, and UL 50, to comply with environmental conditions at installed location.

1. Indoor, Dry and Clean Locations: NEMA 250, Type 1.

2. Other Wet or Damp, Indoor Locations: NEMA 250, Type 4.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Examine elements and surfaces to receive enclosed switches and circuit breakers for compliance with installation tolerances and other conditions affecting performance of the Work.

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

3.2 INSTALLATION

A. Install individual wall-mounted switches and circuit breakers with tops at uniform height unless otherwise indicated.

B. Install fuses in fusible devices.

C. Comply with NECA 1.

3.3 IDENTIFICATION

A. Comply with requirements in Division 26 Section "Identification for Electrical Systems."

1. Identify field-installed conductors, interconnecting wiring, and components; provide warning signs.

2. Label each enclosure with engraved laminated-plastic nameplate.

3.4 FIELD QUALITY CONTROL

A. Testing: Perform inspections, tests, and adjustments.

B. Perform tests and inspections.

1. Inspect components, assemblies, and equipment installations, including connections.

C. Acceptance Testing Preparation:

1. Test insulation resistance for each enclosed switch.

2. Test continuity of each circuit.

D. Tests and Inspections:

1. Perform each visual and mechanical inspection and electrical test stated in NETA Acceptance Testing Specification. Certify compliance with test parameters.

2. Correct malfunctioning units on-site, where possible, and retest to demonstrate compliance; otherwise, replace with new units and retest.

3. Perform the following infrared scan tests and inspections and prepare reports:

a. Initial Infrared Scanning: Perform an infrared scan of each enclosed switch. Remove front panels so joints and connections are accessible to portable scanner.

b. Instruments and Equipment: Use an infrared scanning device designed to measure temperature or to detect significant deviations from normal values. Provide calibration record for device.

E. Enclosed switches and circuit breakers will be considered defective if they do not pass tests and inspections.

F. Prepare test and inspection reports, including a report that identifies enclosed switches and circuit breakers and that describes scanning results. Include notation of deficiencies detected, remedial action taken, and observations after remedial action.

3.5 ADJUSTING

A. Adjust moving parts and operable components to function smoothly, and lubricate as recommended by manufacturer.

***** END OF SECTION *****

SECTION 27 11 00

COMMUNICATIONS EQUIPMENT ROOM FITTINGS

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. Section Includes:

1. Telecommunications mounting elements.
2. Backboards.
3. Telecommunications equipment racks and cabinets.
4. Grounding.

1.3 DEFINITIONS

A. Basket Cable Tray: A fabricated structure consisting of wire mesh bottom and side rails.

B. BICSI: Building Industry Consulting Service International.

C. Channel Cable Tray: A fabricated structure consisting of a one-piece, ventilated-bottom or solid-bottom channel not exceeding 6 inches (152 mm) in width.

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

E. LAN: Local area network.

F. RCDD: Registered Communications Distribution Designer.

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

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

1.4 PERFORMANCE REQUIREMENTS

A. Seismic Performance: Floor-mounted cabinets and cable pathways shall withstand the effects of earthquake motions determined according to [SEI/ASCE 7] <Insert requirement>.

1. The term "withstand" means "the unit will remain in place without separation of any parts from the device when subjected to the seismic forces specified and the unit will be fully operational after the seismic event."

1.5 SUBMITTALS

A. Product Data: For each type of product indicated. Include construction details, material descriptions, dimensions of individual components and profiles, and finishes for equipment racks and cabinets. Include rated capacities, operating characteristics, electrical characteristics, and furnished specialties and accessories.

B. Shop Drawings: For communications equipment room fittings. Include plans, elevations, sections, details, and attachments to other work.

1. Detail equipment assemblies and indicate dimensions, weights, loads, required clearances, method of field assembly, components, and location and size of each field connection.

2. Equipment Racks and Cabinets: Include workspace requirements and access for cable connections.

3. Grounding: Indicate location of grounding bus bar and its mounting detail showing standoff insulators and wall mounting brackets.

C. Qualification Data: For Installer and qualified layout technician, installation supervisor, and field inspector.

D. Seismic Qualification Certificates: For floor-mounted cabinets, accessories, and components, from manufacturer.

1. Basis for Certification: Indicate whether withstand certification is based on actual test of assembled components or on calculation.

2. Dimensioned Outline Drawings of Equipment Unit: Identify center of gravity and locate and describe mounting and anchorage provisions. Base certification on the maximum number of components capable of being mounted in each rack type. Identify components on which certification is based.

3. Detailed description of equipment anchorage devices on which the certification is based and their installation requirements.

1.6 QUALITY ASSURANCE

A. Installer Qualifications: Cabling Installer must have personnel certified by BICSI on staff.

1. Layout Responsibility: Preparation of Shop Drawings shall be under the direct supervision of RCDD/NTS or Commercial Installer, Level 2.

2. Installation Supervision: Installation shall be under the direct supervision of Registered Technician or Level 2 Installer, who shall be present at all times when Work of this Section is performed at Project site.

3. Field Inspector: Currently registered by BICSI as RCDD or Commercial Installer, Level 2 to perform the on-site inspection.

B. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

C. Telecommunications Pathways and Spaces: Comply with TIA/EIA-569-A.

D. Grounding: Comply with ANSI-J-STD-607-A.

1.7 PROJECT CONDITIONS

A. Environmental Limitations: Do not deliver or install equipment frames and cable trays until spaces are enclosed and weathertight, wet work in spaces is complete and dry, and work above ceilings is complete.

1.8 COORDINATION

A. Coordinate layout and installation of communications equipment with Owner's telecommunications and LAN equipment and service suppliers. Coordinate service entrance arrangement with local exchange carrier.

1. Meet jointly with telecommunications and LAN equipment suppliers, local exchange carrier representatives, and Owner to exchange information and agree on details of equipment arrangements and installation interfaces.

2. Record agreements reached in meetings and distribute them to other participants.

3. Adjust arrangements and locations of distribution frames, cross-connects, and patch panels in equipment rooms to accommodate and optimize arrangement and space requirements of LAN equipment.

4. Adjust arrangements and locations of equipment with distribution frames, cross-connects, and patch panels of cabling systems of other communications, electronic safety and security, and related systems that share space in the equipment room.

B. Coordinate location of power raceways and receptacles with locations of communications equipment requiring electrical power to operate.

PART 2 - PRODUCTS

2.1 PATHWAYS

A. General Requirements: Comply with TIA/EIA-569-A.

B. Cable Support: NRTL labeled. Cable support brackets shall be designed to prevent degradation of cable performance and pinch points that could damage cable. Cable tie slots fasten cable ties to brackets.

1. Comply with NFPA 70 and UL 2043 for fire-resistant and low-smoke-producing characteristics.

2. Support brackets with cable tie slots for fastening cable ties to brackets.

3. Lacing bars, spools, J-hooks, and D-rings.

4. Straps and other devices.

C. Conduit and Boxes: Comply with requirements in Division 26 Section "Raceway and Boxes for Electrical Systems." Flexible metal conduit shall not be used.

1. Outlet boxes shall be no smaller than 4 inches wide, 4 inches (75 mm) high, and 2-1/2 inches (64 mm) deep with a single gang plaster ring.

2.2 BACKBOARDS

A. Backboards: Plywood, fire-retardant treated, 3/4 by 48 by 96 inches (19 by 1220 by 2440 mm). Comply with requirements for plywood backing panels specified in Division 06 Section "Rough Carpentry."

2.3 EQUIPMENT FRAMES

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

1. AMP; a Tyco International Ltd. company.

B. General Frame Requirements:

1. Distribution Frames: Freestanding and wall-mounting, modular-steel units designed for telecommunications terminal support and coordinated with dimensions of units to be supported.

2. Module Dimension: Width compatible with EIA 310 standard, 19-inch (480-mm) panel mounting.

3. Finish: Manufacturer's standard, baked-polyester powder coat.

C. Floor-Mounted Racks: Modular-type, steel or aluminum construction.

1. Vertical and horizontal cable management channels, top and bottom cable troughs, grounding lug, and a power strip.

2. Baked-polyester powder coat finish.

D. Modular Freestanding Cabinets:

1. Removable and lockable side panels.
2. Hinged and lockable front and rear doors.
3. Adjustable feet for leveling.
4. Screened ventilation openings in the roof and rear door.
5. Cable access provisions in the roof and base.
6. Grounding bus bar.
7. Rack-mounted, 550-cfm (260-L/s) fan with filter.
8. Power strip.
9. Baked-polyester powder coat finish.
10. All cabinets keyed alike.

E. Cable Management for Equipment Frames:

1. Metal, with integral wire retaining fingers.
2. Baked-polyester powder coat finish.
3. Vertical cable management panels shall have front and rear channels, with covers.
4. Provide horizontal crossover cable manager at the top of each relay rack, with a minimum height of two rack units each.

2.4 POWER STRIPS

A. Power Strips: Comply with UL 1363.

1. Rack mounting.
2. Six 20-A, 120-V ac, NEMA WD 6, Configuration 5-20R receptacles.
3. LED indicator lights for power and protection status.
4. LED indicator lights for reverse polarity and open outlet ground.
5. Circuit Breaker and Thermal Fusing: When protection is lost, circuit opens and cannot be reset.
6. Circuit Breaker and Thermal Fusing: Unit continues to supply power if protection is lost.
7. Cord connected with 15-foot (4.5-m) line cord.
8. Rocker-type on-off switch, illuminated when in on position.
9. Peak Single-Impulse Surge Current Rating: 33 kA per phase.
10. Protection modes shall be line to neutral, line to ground, and neutral to ground. UL 1449 clamping voltage for all 3 modes shall be not more than 330 V.

2.5 GROUNDING

A. Comply with requirements in Division 26 Section "Grounding and Bonding for Electrical Systems." for grounding conductors and connectors.

B. Telecommunications Main Bus Bar:

1. Connectors: Mechanical type, cast silicon bronze, solderless [compression] [exothermic]-type wire terminals, and long-barrel, two-bolt connection to ground bus bar.

2. Ground Bus Bar: Copper, minimum 1/4-inch-thick by 4 inches wide (6 mm thick by 100 mm wide) with 9/32-inch (7.14-mm) holes spaced 1-1/8 inches (28 mm) apart.

3. Stand-Off Insulators: Comply with UL 891 for use in switchboards, 600 V. Lexan or PVC, impulse tested at 5000 V.

C. Comply with ANSI-J-STD-607-A.

2.6 LABELING

A. Comply with TIA/EIA-606-A and UL 969 for a system of labeling materials, including label stocks, laminating adhesives, and inks used by label printers.

PART 3 - EXECUTION

3.1 ENTRANCE FACILITIES

A. Contact telecommunications department and arrange for installation of demarcation point, protected entrance terminals, and a housing.

B. Install underground pathways complying with recommendations in TIA/EIA-569-A, "Entrance Facilities" Article.

3.2 Install underground entrance pathway complying with Division 26 Section "Raceway and Boxes for Electrical Systems. “INSTALLATION.

A. Comply with NECA 1.

B. Comply with BICSI TDMM for layout and installation of communications equipment rooms.

C. Cable Trays: Comply with NEMA VE 2 and TIA/EIA-569-A-7.

D. Bundle, lace, and train conductors and cables to terminal points without exceeding manufacturer's limitations on bending radii. Install lacing bars and distribution spools.

3.3 FIRESTOPPING

A. Comply with requirements in Division 07 Section "Penetration Firestopping." Comply with TIA/EIA-569-A, Annex A, "Firestopping."

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

3.4 GROUNDING

A. Install grounding according to BICSI TDMM, "Grounding, Bonding, and Electrical Protection" Chapter.

B. Comply with ANSI-J-STD-607-A.

C. Locate grounding bus bar to minimize the length of bonding conductors. Fasten to wall allowing at least 2-inch (50-mm) clearance behind the grounding bus bar. Connect grounding bus bar with a minimum No. 4/0 AWG copper grounding electrode conductor from grounding bus bar to electrical building ground point.

D. Bond metallic equipment to the grounding bus bar, using not smaller than No. 6 AWG equipment grounding conductor.

1. Bond the shield of shielded cable to the grounding bus bar in communications rooms and spaces.

3.5 IDENTIFICATION

A. Identify system components, wiring, and cabling complying with TIA/EIA-606-A. Comply with requirements in Division 26 Section "Identification for Electrical Systems." Comply with

requirements in Division 09 Section "Interior Painting" for painting backboards. For fire-resistant plywood, do not paint over manufacturer's label.

B. Labels shall be preprinted or computer-printed type.

***** END OF SECTION *****

SECTION 27 15 00

COMMUNICATIONS HORIZONTAL CABLING

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. Section Includes:

1. Pathways.
2. UTP cabling.
3. Cable connecting hardware, patch panels, and cross-connects.
4. Telecommunications outlet/connectors.
5. Cabling system identification products.
6. Cable management system.

1.3 DEFINITIONS

A. Basket Cable Tray: A fabricated structure consisting of wire mesh bottom and side rails.

B. BICSI: Building Industry Consulting Service International.

C. Channel Cable Tray: A fabricated structure consisting of a one-piece, ventilated-bottom or solid-bottom channel.

D. Consolidation Point: A location for interconnection between horizontal cables extending from building pathways and horizontal cables extending into furniture pathways.

E. Cross-Connect: A facility enabling the termination of cable elements and their interconnection or cross-connection.

F. EMI: Electromagnetic interference.

G. IDC: Insulation displacement connector.

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

I. LAN: Local area network.

J. MUTOA: Multiuser telecommunications outlet assembly, a grouping in one location of several telecommunications outlet/connectors.

K. Outlet/Connectors: A connecting device in the work area on which horizontal cable or outlet cable terminates.

L. RCDD: Registered Communications Distribution Designer.

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

N. Trough or Ventilated Cable Tray: A fabricated structure consisting of longitudinal side rails and a bottom having openings for the passage of air.

O. UTP: Unshielded twisted pair.

1.4 HORIZONTAL CABLING DESCRIPTION

A. Horizontal cable and its connecting hardware provide the means of transporting signals between the telecommunications outlet/connector and the horizontal cross-connect located in the communications equipment room. This cabling and its connecting hardware are called "permanent link," a term that is used in the testing protocols.

1. TIA/EIA-568-B.1 requires that a minimum of two telecommunications outlet/connectors be installed for each work area.

2. Horizontal cabling shall contain no more than one transition point or consolidation point between the horizontal cross-connect and the telecommunications outlet/connector.

3. Bridged taps and splices shall not be installed in the horizontal cabling.

4. Splitters shall not be installed as part of the optical fiber cabling.

B. A work area is approximately 100 sq. ft. (9.3 sq. m), and includes the components that extend from the telecommunications outlet/connectors to the station equipment.

C. The maximum allowable horizontal cable length is 295 feet (90 m). This maximum allowable length does not include an allowance for the length of 16 feet (4.9 m) to the workstation equipment. The maximum allowable length does not include an allowance for the length of 16 feet (4.9 m) in the horizontal cross-connect.

1.5 PERFORMANCE REQUIREMENTS

A. General Performance: Horizontal cabling system shall comply with transmission standards in TIA/EIA-568-B.1, when tested according to test procedures of this standard.

1.6 SUBMITTALS

A. Product Data: For each type of product indicated.

1. For coaxial cable, include the following installation data for each type used:

a. Nominal OD.

b. Minimum bending radius.

c. Maximum pulling tension.

B. Shop Drawings:

1. System Labeling Schedules: Electronic copy of labeling schedules, in software and format selected by Owner.

2. System Labeling Schedules: Electronic copy of labeling schedules that are part of the cabling and asset identification system of the software.

3. Cabling administration drawings and printouts.

4. Wiring diagrams to show typical wiring schematics, including the following:

a. Cross-connects.

b. Patch panels.

c. Patch cords.

5. Cross-connects and patch panels. Detail mounting assemblies, and show elevations and physical relationship between the installed components.

6. Cable tray layout, showing cable tray route to scale, with relationship between the tray and adjacent structural, electrical, and mechanical elements. Include the following:

a. Vertical and horizontal offsets and transitions.

b. Clearances for access above and to side of cable trays.

c. Vertical elevation of cable trays above the floor or bottom of ceiling structure.

d. Load calculations to show dead and live loads as not exceeding manufacturer's rating for tray and its support elements.

C. Samples: For workstation outlets, jacks, jack assemblies, in specified finish, one for each size and outlet configuration and faceplates for color selection and evaluation of technical features.

D. Qualification Data: For Installer and qualified layout technician, installation supervisor, and field inspector.

E. Source quality-control reports.

F. Field quality-control reports.

G. Maintenance Data: For splices and connectors to include in maintenance manuals.

H. Software and Firmware Operational Documentation:

1. Software operating and upgrade manuals.

2. Program Software Backup: On magnetic media or compact disk, complete with data files.

3. Device address list.

4. Printout of software application and graphic screens.

1.7 QUALITY ASSURANCE

A. Installer Qualifications: Cabling Installer must have personnel certified by BICSI on staff.

1. Layout Responsibility: Preparation of Shop Drawings and Cabling Administration Drawings, Cabling Administration Drawings, and field testing program development by an RCDD.

2. Installation Supervision: Installation shall be under the direct supervision of Registered Technician or Level 2 Installer, who shall be present at all times when Work of this Section is performed at Project site.

3. Testing Supervisor: Currently certified by BICSI as an RCDD to supervise on-site testing.

B. Testing Agency Qualifications: An NRTL.

1. Testing Agency's Field Supervisor: Currently certified by BICSI as an RCDD to supervise on-site testing.

C. Surface-Burning Characteristics: As determined by testing identical products according to ASTM E 84 by a qualified testing agency. Identify products with appropriate markings of applicable testing agency.

1. Flame-Spread Index: 25 or less.

2. Smoke-Developed Index: 450 or less.

D. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

E. Telecommunications Pathways and Spaces: Comply with TIA/EIA-569-A.

F. Grounding: Comply with ANSI-J-STD-607-A.

1.8 DELIVERY, STORAGE, AND HANDLING

A. Test cables upon receipt at Project site.

1. Test each pair of UTP cable for open and short circuits.

1.9 PROJECT CONDITIONS

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

1.10 COORDINATION

A. Coordinate layout and installation of telecommunications pathways and cabling with Owner's telecommunications and LAN equipment and service suppliers.

B. Coordinate telecommunications outlet/connector locations with location of power receptacles at each work area.

1.11 SOFTWARE SERVICE AGREEMENT

A. Technical Support: Beginning with Substantial Completion, provide software support for two years.

B. Upgrade Service: Update software to latest version at Project completion. Install and program software upgrades that become available within two years from date of Substantial Completion. Upgrading software shall include operating system. Upgrade shall include new or revised licenses for use of software.

1. Provide 30 days' notice to Owner to allow scheduling and access to system and to allow Owner to upgrade computer equipment if necessary.

1.12 EXTRA MATERIALS

A. Furnish extra materials that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.

1. Patch-Panel Units: One of each type.

2. Device Plates: Ten of each type.

PART 2 - PRODUCTS

2.1 PATHWAYS

A. General Requirements: Comply with TIA/EIA-569-A.

B. Cable Support: NRTL labeled for support of Category 6 cabling, designed to prevent degradation of cable performance and pinch points that could damage cable.

1. Support brackets with cable tie slots for fastening cable ties to brackets.

2. Lacing bars, spools, J-hooks, and D-rings.

3. Straps and other devices.

2.2 BACKBOARDS

A. Backboards: Plywood, fire-retardant treated, 3/4 by 48 by 96 inches (19 by 1220 by 2440 mm). Comply with requirements in Division 06 Section "Rough Carpentry" for plywood backing panels.

2.3 UTP CABLE

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

1. Berk-Tek; a Nexans company.

B. Description: 100-ohm, 4-pair UTP covered with a yellow thermoplastic jacket.

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

2.4 UTP CABLE HARDWARE

A. Manufacturers: Subject to compliance with requirements, provide products by the following manufacturer:
    1. Tyco Electronics/AMP Netconnect; Tyco International Ltd.

B. General Requirements for Cable Connecting Hardware: Comply with TIA/EIA-568-B.2, IDC type, with modules designed for punch-down caps or tools. Cables shall be terminated with connecting hardware of same category or higher.

C. Patch Panel: Modular panels housing multiple-numbered jack units with IDC-type connectors at each jack for permanent termination of pair groups of installed cables.
    1. Number of Jacks per Field: One for each four-pair UTP cable indicated plus spares and blank positions adequate to suit specified expansion criteria].

D. Jacks and Jack Assemblies: Modular, color-coded, eight-position modular receptacle units with integral IDC-type terminals.

E. Patch Cords: Factory-made, four-pair cables in 36-inch (900 mm) and 48-inch (1200-mm) lengths; terminated with eight-position modular plug at each end.
    1. Patch cords shall have bend-relief-compliant boots and color-coded icons to ensure Category 6 performance. Patch cords shall have latch guards to protect against snagging.
    2. Patch cords shall have color-coded boots for circuit identification.

2.5 TELECOMMUNICATIONS OUTLET/CONNECTORS

A. Jacks: 100-ohm, balanced, twisted-pair connector; four-pair, eight-position modular. Comply with TIA/EIA-568-B.1.

B. Workstation Outlets: Two port-connector assemblies mounted in single or multigang faceplate.
    1. Plastic Faceplate: High-impact plastic. Coordinate color with Division 26 Section "Wiring Devices."
    2. For use with snap-in jacks accommodating any combination of UTP, optical fiber, and coaxial work area cords.
        a. Flush mounting jacks, positioning the cord at a 45-degree angle.
    3. Legend: Snap-in, clear-label covers and machine-printed paper inserts.

2.6 GROUNDING

A. Comply with requirements in Division 26 Section "Grounding and Bonding for Electrical Systems" for grounding conductors and connectors.

B. Comply with ANSI-J-STD-607-A.

2.7 IDENTIFICATION PRODUCTS

A. Comply with TIA/EIA-606-A and UL 969 for labeling materials, including label stocks, laminating adhesives, and inks used by label printers.

B. Comply with requirements in Division 26 Section "Identification for Electrical Systems."

2.8 CABLE MANAGEMENT SYSTEM

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. iTRACS Corporation.

2. Telsoft Solutions.

B. Description: Computer-based cable management system, with integrated database and graphic capabilities.

C. Document physical characteristics by recording the network, TIA/EIA details, and connections between equipment and cable.

D. Information shall be presented in database view, schematic plans, or technical drawings.

1. AutoCAD drawing software shall be used as drawing and schematic plans software.

E. System shall interface with the following testing and recording devices:

1. Direct upload tests from circuit testing instrument into the personal computer.

2. Direct download circuit labeling into labeling printer.

2.9 SOURCE QUALITY CONTROL

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

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

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

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

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

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

G. Prepare test and inspection reports.

PART 3 - EXECUTION

3.1 ENTRANCE FACILITIES

A. Coordinate backbone cabling with the protectors and demarcation point provided by communications service provider.

3.2 WIRING METHODS

A. Wiring Method: Install cables in raceways except within consoles, cabinets, desks, counters and accessible ceiling spaces. Conceal raceway and cables except in unfinished spaces.

1. Install plenum cable in environmental air spaces, including plenum ceilings.

2. Comply with requirements for raceways and boxes specified in Division 26 Section "Raceway and Boxes for Electrical Systems."

B. Wiring Method: Conceal conductors and cables in accessible ceilings, walls, and floors where possible.

C. Wiring within Enclosures: Bundle, lace, and train cables to terminal points with no excess and without exceeding manufacturer's limitations on bending radii. Provide and use lacing bars and distribution spools.

3.3 INSTALLATION OF PATHWAYS

A. Comply with requirements for demarcation point, pathways, cabinets, and racks specified in Division 27 Section "Communications Equipment Room Fittings." Drawings indicate general arrangement of pathways and fittings.

B. Comply with TIA/EIA-569-A for pull-box sizing and length of conduit and number of bends between pull points.

C. Comply with requirements in Division 26 Section "Raceway and Boxes for Electrical Systems" for installation of conduits and wireways.

D. Install manufactured conduit sweeps and long-radius elbows whenever possible.

E. Pathway Installation in Communications Equipment Rooms:

1. Position conduit ends adjacent to a corner on backboard where a single piece of plywood is installed, or in the corner of room where multiple sheets of plywood are installed around perimeter walls of room.

2. Install cable trays to route cables if conduits cannot be located in these positions.

3. Secure conduits to backboard when entering room from overhead.

4. Extend conduits 3 inches (76 mm) above finished floor.

5. Install metal conduits with grounding bushings and connect with grounding conductor to grounding system.

F. Backboards: Install backboards with 96-inch (2440-mm) dimension vertical. Butt adjacent sheets tightly, and form smooth gap-free corners and joints.

3.4 INSTALLATION OF CABLES

A. Comply with NECA 1.

B. General Requirements for Cabling:

1. Comply with TIA/EIA-568-B.1.

2. Comply with BICSI ITSIM, Ch. 6, "Cable Termination Practices."

3. Install 110-style IDC termination hardware unless otherwise indicated.

4. Terminate conductors; no cable shall contain unterminated elements. Make terminations only at indicated outlets, terminals, cross-connects, and patch panels.

5. Cables may not be spliced. Secure and support cables at intervals not exceeding 30 inches (760 mm) and not more than 6 inches (150 mm) from cabinets, boxes, fittings, outlets, racks, frames, and terminals.

6. Install lacing bars to restrain cables, to prevent straining connections, and to prevent bending cables to smaller radii than minimums recommended by manufacturer.

7. Bundle, lace, and train conductors to terminal points without exceeding manufacturer's limitations on bending radii, but not less than radii specified in BICSI ITSIM, "Cabling Termination Practices" Chapter. Install lacing bars and distribution spools.

8. Do not install bruised, kinked, scored, deformed, or abraded cable. Do not splice cable between termination, tap, or junction points. Remove and discard cable if damaged during installation and replace it with new cable.

9. Cold-Weather Installation: Bring cable to room temperature before dereeling. Heat lamps shall not be used for heating.

10. In the communications equipment room, install a 10-foot- (3-m-) long service loop on each end of cable.

11. Pulling Cable: Comply with BICSI ITSIM, Ch. 4, "Pulling Cable." Monitor cable pull tensions.

C. UTP Cable Installation:

1. Comply with TIA/EIA-568-B.2.

2. Do not untwist UTP cables more than 1/2 inch (12 mm) from the point of termination to maintain cable geometry.

D. Open-Cable Installation:

1. Install cabling with horizontal and vertical cable guides in telecommunications spaces with terminating hardware and interconnection equipment.

2. Suspend UTP cable not in a wireway or pathway a minimum of 8 inches (200 mm) above ceilings by cable supports not more than 60 inches (1524 mm) apart.

3. Cable shall not be run through structural members or in contact with pipes, ducts, or other potentially damaging items.

E. Installation of Cable Routed Exposed under Raised Floors:

1. Install plenum-rated cable only.

2. Install cabling after the flooring system has been installed in raised floor areas.

3. Coil cable [6 feet (1800 mm)] <Insert size> long not less than [12 inches (300 mm)] <Insert size> in diameter below each feed point.

F. Outdoor Coaxial Cable Installation:

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

2. Attach antenna lead-in cable to support structure at intervals not exceeding 36 inches (915 mm).

G. Group connecting hardware for cables into separate logical fields.

H. Separation from EMI Sources:

1. Comply with BICSI TDMM and TIA/EIA-569-A for separating unshielded copper voice and data communication cable from potential EMI sources, including electrical power lines and equipment.

2. Separation between open communications cables or cables in nonmetallic raceways and unshielded power conductors and electrical equipment shall be as follows:

a. Electrical Equipment Rating Less Than 2 kVA: A minimum of 5 inches (127 mm).

b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 12 inches (300 mm).

c. Electrical Equipment Rating More Than 5 kVA: A minimum of 24 inches (610 mm).

3. Separation between communications cables in grounded metallic raceways and unshielded power lines or electrical equipment shall be as follows:

   a. Electrical Equipment Rating Less Than 2 kVA: A minimum of 2-1/2 inches (64 mm).

   b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 6 inches (150 mm).

   c. Electrical Equipment Rating More Than 5 kVA: A minimum of 12 inches (300 mm).

4. Separation between communications cables in grounded metallic raceways and power lines and electrical equipment located in grounded metallic conduits or enclosures shall be as follows:

   a. Electrical Equipment Rating Less Than 2 kVA: No requirement.

   b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 3 inches (76 mm).

   c. Electrical Equipment Rating More Than 5 kVA: A minimum of 6 inches (150 mm).

5. Separation between Communications Cables and Electrical Motors and Transformers, 5 kVA or HP and Larger: A minimum of 48 inches (1200 mm).

6. Separation between Communications Cables and Fluorescent Fixtures: A minimum of 5 inches (127 mm).

3.5 FIRESTOPPING

A. Comply with requirements in Division 07 Section "Penetration Firestopping."

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

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

3.6 GROUNDING

A. Install grounding according to BICSI TDMM, "Grounding, Bonding, and Electrical Protection" Chapter.

B. Comply with ANSI-J-STD-607-A.

C. Locate grounding bus bar to minimize the length of bonding conductors. Fasten to wall allowing at least 2-inch (50-mm) clearance behind the grounding bus bar. Connect grounding bus bar with a minimum No. 4 AWG grounding electrode conductor from grounding bus bar to suitable electrical building ground.

D. Bond metallic equipment to the grounding bus bar, using not smaller than No. 6 AWG equipment grounding conductor.

3.7 IDENTIFICATION

A. Identify system components, wiring, and cabling complying with TIA/EIA-606-A. Comply with requirements for identification specified in Division 26 Section "Identification for Electrical Systems."

   1. Administration Class: 1.

   2. Color-code cross-connect fields. Apply colors to voice and data service backboards, connections, covers, and labels.

B. Using cable management system software specified in Part 2, develop Cabling Administration Drawings for system identification, testing, and management. Use unique, alphanumeric designation for each cable and label cable, jacks, connectors, and terminals to which it

connects with same designation. At completion, cable and asset management software shall reflect as-built conditions.

C. Comply with requirements in Division 09 Section "Interior Painting" for painting backboards. For fire-resistant plywood, do not paint over manufacturer's label.

D. Paint and label colors for equipment identification shall comply with TIA/EIA-606-A for Class 2 level of administration, including optional identification requirements of this standard.

E. Cable Schedule: Post in prominent location in each equipment room and wiring closet. List incoming and outgoing cables and their designations, origins, and destinations. Protect with rigid frame and clear plastic cover. Furnish an electronic copy of final comprehensive schedules for Project.

F. Cabling Administration Drawings: Show building floor plans with cabling administration-point labeling. Identify labeling convention and show labels for telecommunications closets, backbone pathways and cables, entrance pathways and cables, terminal hardware and positions, horizontal cables, work areas and workstation terminal positions, grounding buses and pathways, and equipment grounding conductors. Follow convention of TIA/EIA-606-A. Furnish electronic record of all drawings, in software and format selected by Owner.

G. Cable and Wire Identification:

1. Label each cable within 4 inches (100 mm) of each termination and tap, where it is accessible in a cabinet or junction or outlet box, and elsewhere as indicated.

2. Each wire connected to building-mounted devices is not required to be numbered at device if color of wire is consistent with associated wire connected and numbered within panel or cabinet.

3. Exposed Cables and Cables in Cable Trays and Wire Troughs: Label each cable at intervals not exceeding 15 feet (4.5 m).

4. Label each terminal strip and screw terminal in each cabinet, rack, or panel.

a. Individually number wiring conductors connected to terminal strips, and identify each cable or wiring group being extended from a panel or cabinet to a building-mounted device shall be identified with name and number of particular device as shown.

b. Label each unit and field within distribution racks and frames.

5. Identification within Connector Fields in Equipment Rooms and Wiring Closets: Label each connector and each discrete unit of cable-terminating and connecting hardware. Where similar jacks and plugs are used for both voice and data communication cabling, use a different color for jacks and plugs of each service.

H. Labels shall be preprinted or computer-printed type with printing area and font color that contrasts with cable jacket color but still complies with requirements in TIA/EIA-606-A.

1. Cables use flexible vinyl or polyester that flex as cables are bent.

3.8 FIELD QUALITY CONTROL

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

B. Perform tests and inspections.

C. Tests and Inspections:

1. Visually inspect UTP and optical fiber cable jacket materials for NRTL certification markings. Inspect cabling terminations in communications equipment rooms for compliance with color-coding for pin assignments, and inspect cabling connections for compliance with TIA/EIA-568-B.1.

2. Visually confirm Category 6, marking of outlets, cover plates, outlet/connectors, and patch panels.

3. Visually inspect cable placement, cable termination, grounding and bonding, equipment and patch cords, and labeling of all components.

4. Test UTP backbone copper cabling for DC loop resistance, shorts, opens, intermittent faults, and polarity between conductors. Test operation of shorting bars in connection blocks. Test cables after termination but not cross-connection.

    a. Test instruments shall meet or exceed applicable requirements in TIA/EIA-568-B.2. Perform tests with a tester that complies with performance requirements in "Test Instruments (Normative)" Annex, complying with measurement accuracy specified in "Measurement Accuracy (Informative)" Annex. Use only test cords and adapters that are qualified by test equipment manufacturer for channel or link test configuration.

5. Optical Fiber Cable Tests:

    a. Test instruments shall meet or exceed applicable requirements in TIA/EIA-568-B.1. Use only test cords and adapters that are qualified by test equipment manufacturer for channel or link test configuration.

    b. Link End-to-End Attenuation Tests:

        1) Horizontal and multimode backbone link measurements: Test at 850 or 1300 nm in 1 direction according to TIA/EIA-526-14-A, Method B, One Reference Jumper.

        2) Attenuation test results for backbone links shall be less than 2.0 dB. Attenuation test results shall be less than that calculated according to equation in TIA/EIA-568-B.1.

6. UTP Performance Tests:

    a. Test for each outlet. Perform the following tests according to TIA/EIA-568-B.1 and TIA/EIA-568-B.2:

        1) Wire map.

        2) Length (physical vs. electrical, and length requirements).

        3) Insertion loss.

        4) Near-end crosstalk (NEXT) loss.

        5) Power sum near-end crosstalk (PSNEXT) loss.

        6) Equal-level far-end crosstalk (ELFEXT).

        7) Power sum equal-level far-end crosstalk (PSELFEXT).

        8) Return loss.

        9) Propagation delay.

        10) Delay skew.

7. Optical Fiber Cable Performance Tests: Perform optical fiber end-to-end link tests according to TIA/EIA-568-B.1 and TIA/EIA-568-B.3.

8. Coaxial Cable Tests: Conduct tests according to Division 27 Section "Master Antenna Television System."

9. Final Verification Tests: Perform verification tests for UTP systems after the complete communications cabling and workstation outlet/connectors are installed.

a. Data Tests: These tests assume the Information Technology Staff has a network installed and is available to assist with testing. Connect to the network interface device at the demarcation point. Log onto the network to ensure proper connection to the network.

D. Document data for each measurement. Data for submittals shall be printed in a summary report that is formatted similar to Table 10.1 in BICSI TDMM, or transferred from the instrument to the computer, saved as text files, and printed and submitted.

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

F. Prepare test and inspection reports.

3.9 DEMONSTRATION

A. Engage a factory-authorized service representative to train Owner's maintenance personnel in cable-plant management operations, including changing signal pathways for different workstations, rerouting signals in failed cables, and keeping records of cabling assignments and revisions when extending wiring to establish new workstation outlets. Include training in cabling administration software.

***** END OF SECTION *****

SECTION 28 13 00

ACCESS CONTROL

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. Section Includes:

1. Security access central-control station.

2. Security access operating system and application software.

1.3 DEFINITIONS

A. CCTV: Closed-circuit television.

B. CPU: Central processing unit.

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

D. dpi: Dots per inch.

E. DTS: Digital Termination Service. A microwave-based, line-of-sight communication provided directly to the end user.

F. GFI: Ground fault interrupter.

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

H. I/O: Input/Output.

I. LAN: Local area network.

J. Location: A Location on the network having a PC-to-controller communications link, with additional controllers at the Location connected to the PC-to-controller link with a TIA 485-A communications loop. Where this term is presented with an initial capital letter, this definition applies.

K. PC: Personal computer. Applies to the central station, workstations, and file servers.

L. PCI Bus: Peripheral Component Interconnect. A peripheral bus providing a high-speed data path between the CPU and the peripheral devices such as a monitor, disk drive, or network.

M. PDF: Portable Document Format. The file format used by the Acrobat document-exchange-system software from Adobe.

N. RAS: Remote access services.

O. RF: Radio frequency.

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

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

R. TWAIN: Technology without an Interesting Name. A programming interface that lets a graphics application, such as an image editing program or desktop publishing program, activate a scanner, frame grabber, or other image-capturing device.

S. UPS: Uninterruptible power supply.

T. USB: Universal serial bus.

U. WAN: Wide area network.

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

W. WMP: Windows media player.

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

Y. Windows: Operating system by Microsoft Corporation.

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

AA. WYSIWYG: What You See Is What You Get. Text and graphics appear on the screen the same as they will in print.

1.4 SUBMITTALS

A. Product Data: For each type of product indicated. Include rated capacities, operating characteristics, and furnished specialties and accessories. Reference each product to a location on Drawings. Test and evaluation data presented in Product Data shall comply with SIA BIO-01.

B. Shop Drawings: Include plans, elevations, sections, details, and attachments to other work.

1. Diagrams for cable management system.

2. System labeling schedules, including electronic copy of labeling schedules that are part of the cable and asset identification system of the software specified in Parts 2 and 3.

3. Wiring Diagrams. For power, signal, and control wiring. Show typical wiring schematics including the following:

a. Workstation outlets, jacks, and jack assemblies.

b. Patch cords.

c. Patch panels.

4. Cable Administration Drawings: As specified in "Identification" Article.

5. Battery and charger calculations for central station, workstations, and controllers.

C. Samples: For workstation outlets, jacks, jack assemblies, and faceplates. For each exposed product and for each color and texture specified.

D. Other Action Submittals:

1. Project planning documents as specified in Part 3.

E. Field quality-control reports.

F. Operation and Maintenance Data: For security system to include in emergency, operation, and maintenance manuals. In addition to items specified in Division 01 Section "Operation and Maintenance Data," include the following:

1. Microsoft Windows software documentation.

2. PC installation and operating documentation, manuals, and software for the PC and all installed peripherals. Software shall include system restore, emergency boot diskettes, and drivers for all installed hardware. Provide separately for each PC.

3. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on CD-ROM of the hard-copy submittal.

4. System installation and setup guides with data forms to plan and record options and setup decisions.

1.5 QUALITY ASSURANCE

A. Installer Qualifications: An employer of workers trained and approved by manufacturer.

1. Cable installer must have on staff a registered communication distribution designer certified by Building Industry Consulting Service International.

B. Source Limitations: Obtain central station, workstations, controllers, Identifier readers, and all software through one source from single manufacturer.

C. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

D. Comply with NFPA 70, "National Electrical Code."

E. Comply with SIA DC-01 and SIA DC-03 and SIA DC-07.

1.6 DELIVERY, STORAGE, AND HANDLING

A. Central Station, Workstations, and Controllers:

1. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85 deg F (10 and 30 deg C), and not more than 80 percent relative humidity, noncondensing.

2. Open each container; verify contents against packing list; and file copy of packing list, complete with container identification, for inclusion in operation and maintenance data.

3. Mark packing list with the same designations assigned to materials and equipment for recording in the system labeling schedules that are generated by software specified in "Cable and Asset Management Software" Article.

4. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.7 PROJECT CONDITIONS

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

1. Control Station: Rated for continuous operation in ambient conditions of 60 to 85 deg F (16 to 30 deg C) and a relative humidity of 20 to 80 percent, noncondensing.

2. Indoor, Controlled Environment: NEMA 250, Type 1 enclosure. System components, except the central-station control unit, installed in air-conditioned indoor environments shall be rated for continuous operation in ambient conditions of 36 to 122 deg F (2 to 50 deg C) dry bulb and 20 to 90 percent relative humidity, noncondensing.

3. Indoor, Uncontrolled Environment: NEMA 250, Type 3R enclosures. System components installed in non-air-conditioned indoor environments shall be rated for continuous operation in ambient conditions of 0 to 122 deg F (minus 18 to plus 50 deg C) temperature range> dry bulb and 20 to 90 percent relative humidity, noncondensing.

4. Outdoor Environment: NEMA 250, NEMA 250, Type 3R enclosures. System components installed in locations exposed to weather shall be rated for continuous operation in ambient conditions of minus 30 to plus 122 deg F (minus 34 to plus 50 deg C) dry bulb and 20 to 90 percent relative humidity, condensing. Rate for continuous operation where exposed to rain as specified in NEMA 250, winds up to 110 mph.

B. Furnish extra materials that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.

1. Alarm Printer Black/Red Ribbons: Package of 12.

2. Laser Printers: Three toner cassettes and one replacement drum unit.

3. Credential card blanks, ready for printing. Include enough credential cards for all personnel to be enrolled at the site plus an extra 50 percent for future use.

4. Fuses of all kinds, power and electronic, equal to 10 percent of amount installed for each size used, but no fewer than three units.

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. ABM Data Systems, Inc.

2. Alco Advanced Technologies.

3. Bosch Security Systems, Inc.

4. Checkpoint Systems, Inc.

5. Continental Instruments; a NAPCO Security Group company.

6. Deister Electronic USA, Inc.

7. Galaxy Control Systems.

8. General Electric Company; GE Security, Inc.

9. HES; an ASSA ABLOY Group company.

10. Hirsch Electronics Corporation.

11. Honeywell International Inc; Honeywell Access Systems.

12. Honeywell International Inc; Honeywell Integrated Security (formerly: NexWatch).

13. Keyscan.

14. Matrix Systems, Inc.

15. Secura Key.

16. TAC; Andover Continuum Brand.

2.2 DESCRIPTION

A. Security Access System: PC-based central station, one or more networked PC-based workstations, and field-installed controllers, connected by a high-speed electronic-data transmission network.

B. System Software: Based on 32-bit, Microsoft Windows central-station and workstation operating system and application software.

C. Workstation operating system, server operating system, and application software. Software shall have the following capabilities:

1. Multiuser and multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations.
2. Graphical user interface to show pull-down menus and a menu-tree format that complies with interface guidelines of Microsoft Windows.
3. System license for the entire system including capability for future additions that are within the indicated system size limits specified in this Section.
4. Open-architecture system that allows importing and exporting of data and interfacing with other systems that are compatible with Microsoft Windows.
5. Password-protected operator login and access.
6. Open-database-connectivity compliant.

D. Network connecting the central station and workstations shall be a WAN using Microsoft Windows-based TCP/IP with a capacity of connecting up to 99 workstations. System shall be portable across multiple communication platforms without changing system software.

E. Network(s) connecting PCs and controllers shall consist of one or more of the following:

1. Local area, IEEE 802.3 Fast Ethernet Gigabit-Ethernet, star topology network based on TCP/IP.
2. Direct-connected, RS-232 cable from the COM port of the central station to the first controller, then RS-485 cable to interconnect the remaining controllers at that Location.
3. Dial-up and cable modem connection using a standard cable or dial-up telephone line.

2.3 OPERATION

A. Security access system shall use a single database for access-control and credential-creation functions.

B. Distributed Processing: A fully distributed processing system.

1. Access-control information, including time, date, valid codes, access levels, and similar data, shall be downloaded to controllers so each controller can make access-control decisions.
2. Intermediate controllers for access control are prohibited.
3. In the event that communications with the central controller are lost, controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the central station.

C. Data Capacity:

1. 130 different card-reader formats.
2. 999 comments.
3. 48 graphic file types for importing maps.

D. Location Capacity:

1. 128 reader-controlled doors.
2. 50,000 total-access credentials.
3. 2048 supervised alarm inputs.
4. 2048 programmable outputs.

5. 32,000 custom action messages per Location to instruct operator on action required when alarm is received.

E. System Network Requirements:

1. System components shall be interconnected and shall provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.

2. Communication shall not require operator initiation or response and shall return to normal after partial- or total-network interruption such as power loss or transient upset.

3. System shall automatically annunciate communication failures to the operator and shall identify the communications link that has experienced a partial or total failure.

4. Communications controller may be used as an interface between the central-station display systems and the field device network. Communications controller shall provide functions required to attain the specified network communications performance.

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

G. Field equipment shall include controllers, sensors, and controls.

1. Controllers shall serve as an interface between the central station and sensors and controls.

2. Data exchange between the central station and the controllers shall include down-line transmission of commands, software, and databases to controllers.

3. The up-line data exchange from the controller to the central station shall include status data such as intrusion alarms, status reports, and entry-control records.

4. Controllers are classified as alarm-annunciation or entry-control type.

H. System Response to Alarms:

1. Field device network shall provide a system end-to-end response time of one second or less for every device connected to the system.

2. Alarms shall be annunciated at the central station within one second of the alarm occurring at a controller or at a device controlled by a local controller, and within 100 ms if the alarm occurs at the central station.

3. Alarm and status changes shall be displayed within 100 ms after receipt of data by the central station.

4. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within five seconds of alarm receipt at the security console.

5. This response time shall be maintained during system heavy load.

I. False-Alarm Reduction: The design of the central station and controllers shall contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.

J. Error Detection:

1. Use a cyclic code method to detect single- and double-bit errors, burst errors of eight bits or fewer, and at least 99 percent of all other multibit and burst errors between controllers and the central station.

2. Interactive or product error-detection codes alone will not be acceptable.

3. A message shall be in error if one bit is received incorrectly.

4. Retransmit messages with detected errors.

5. Allow for an operator-assigned two-digit decimal number to each communications link representing the number of retransmission attempts.

6. Central station shall print a communication failure alarm message when the number of consecutive retransmission attempts equals the assigned quantity.

7. Monitor the frequency of data transmission failure for display and logging.

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

L. Door Hardware Interface:

1. Comply with requirements in Division 08 Sections for door hardware required to be monitored or controlled by the security access system.

2. Electrical characteristics of controllers shall match the signal and power requirements of door hardware.

2.4 APPLICATION SOFTWARE

A. System Software: Based on 32-bit, Microsoft Windows central-station and workstation operating system and application software.

1. Multiuser multitasking shall allow independent activities and monitoring to occur simultaneously at different workstations.

2. Graphical user interface shall show pull-down menus and a menu-tree format.

3. Capability for future additions within the indicated system size limits.

4. Open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with operating system.

5. Password-protected operator login and access.

B. Peer Computer Control Software: Detect a failure of a central computer and cause the other central computer to assume control of all system functions without interruption of operation. Both central computers shall have drivers to support this mode of operation.

C. Application Software: Interface between the alarm annunciation and entry-control controllers to monitor sensors and DTS links, operate displays, report alarms, generate reports, and help train system operators.

1. Reside at the central station, workstations, and controllers as required to perform specified functions.

2. Operate and manage peripheral devices.

3. Manage files for disk I/O, including creating, deleting, and copying files; and automatically maintain a directory of all files, including size and location of each sequential and random-ordered record.

4. Import custom icons into graphics to represent alarms and I/O devices.

5. Globally link I/O so that any I/O can link to any other I/O within the same Location without requiring interaction with the host PC. This operation shall be at the controller.

6. Globally code I/O links so that any access-granted event can link to any I/O with the same Location without requiring interaction with the host PC. This operation shall be at the controller.

7. Messages from PC to controllers and controllers to controllers shall be on a polled network that utilizes check summing and acknowledgment of each message.

Communication shall be automatically verified, buffered, and retransmitted if message is not acknowledged.

8. Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-controller communications methods by changing the polling frequency and the amount of time the system waits for a response.

9. Automatic and encrypted backups for database and history backups shall be automatically stored at the central-control PC and encrypted with a nine-character alphanumeric password that must be used to restore or read data contained in backup.

10. Operator audit trail for recording and reporting all changes made to database and system software.

11. Support network protocol and topology, TCP/IP, Novel Netware, Digital Pathworks, Banyan Vines, LAN/WAN, and RAS.

D. Workstation Software:

1. Password levels shall be individually customized at each workstation to allow or disallow operator access to program functions for each Location.

2. Workstation event filtering shall allow user to define events and alarms that will be displayed at each workstation. If an alarm is unacknowledged (not handled by another workstation) for a preset amount of time, the alarm will automatically appear on the filtered workstation.

E. Controller Software:

1. The controller shall operate as autonomous, intelligent processing units.

a. The controller shall make decisions about access control, alarm monitoring, linking functions, and door-locking schedules for their operation, independent of other system components.

b. The portion of the database associated with a controller, and consisting of parameters, constraints, and the latest value or status of points connected to that controller, shall be maintained in the controller.

2. The following functions shall be fully implemented and operational within the controller:

a. Monitoring inputs.

b. Controlling outputs.

c. Automatically reporting alarms to the central station.

d. Reporting of sensor and output status to the central station on request.

e. Maintaining real time, automatically updated by the central station at least once a day.

f. Executing controller resident programs.

g. Diagnosing.

3. Controller Operation:

a. Storage capacity for the latest 1024 events shall be provided at the controller.

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

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

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

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

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

g. After power is restored, following a power failure, startup software shall initiate self-test diagnostic routines, after which the controller shall resume normal operation.

h. After controller failure, if the database and application software are no longer resident, controllers shall not restart but shall remain in the failure mode until repaired. If database and application programs are resident, controllers shall immediately resume operation. If not, software shall be restored automatically from the central station.

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

F. PC-to-Controller Communications:

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

a. Direct connection using serial ports of the PC.

b. TCP/IP LAN interface cards.

c. Dial-up or cable modems for connections to Locations.

2. Each serial port used for communications shall be individually configurable for "direct communications," "modem communications incoming and outgoing," or "modem communications incoming only," or as an ASCII output port. Serial ports shall have adjustable data transmission rates and shall be selectable under program control.

3. Use multiport communications board if more than two serial ports are needed.

a. Use a 4-, 8-, or 16-serial port configuration that is expandable to 32- or 64-serial ports.

b. Connect the first board to an internal PCI bus adapter card.

4. Direct serial, TCP/IP, and dial-up, cable, or satellite communications shall be alike in the monitoring or control of the system except for the connection that must first be made to a dial-up or voice-over IP Location.

5. TCP/IP network interface card (NIV) shall have an option to set the poll-frequency and message-response time-out settings.

6. PC-to-controller and controller-to-controller communications (direct, dial-up, or TCP/IP) shall use a polled-communication protocol that checks sum and acknowledges each message. All communications in this subparagraph shall be verified and buffered, and retransmitted if not acknowledged.

G. Direct Serial or TCP/IP PC-to-Controller Communications:

1. Communication software on the PC shall supervise the PC-to-controller communications link.
2. Loss of communications to any controller shall result in an alarm at all PCs running the communication software.
3. When communications are restored, all buffered events shall automatically upload to the PC, and any database changes shall be automatically sent to the controller.

H. Operator Interface:

1. Inputs in system shall have two icon representations, one for the normal state and one for the abnormal state.
2. When viewing and controlling inputs, displayed icons shall automatically change to the proper icon to display the current system state in real time. Icons shall also display the input's state, whether armed or bypassed, and if the input is in the armed or bypassed state due to a time zone or a manual command.
3. Outputs in system shall have two icon representations, one for the secure (locked) state and one for the open (unlocked) state.
4. Icons displaying status of the I/O points shall be constantly updated to show their current real-time condition without prompting by the operator.
5. The operator shall be able to scroll the list of I/Os and press the appropriate toolbar button, or right click, to command the system to perform the desired function.
6. Override Groups Containing I/Os:
    a. System shall incorporate override groups that provide the operator with the status and control over user-defined "sets" of I/Os with a single icon.
    b. Icon shall change automatically to show the live summary status of points in that group.
    c. Override group icon shall provide a method to manually control or set to time-zone points in the group.
    d. Override group icon shall allow the expanding of the group to show icons representing the live status for each point in the group, individual control over each point, and the ability to compress the individual icons back into one summary icon.
7. Schedule Overrides of I/Os and Override Groups:
    a. To accommodate temporary schedule changes that do not fall within the holiday parameters, the operator shall have the ability to override schedules individually for each input, output, or override group.
    b. Each schedule shall be composed of a minimum of two dates with separate times for each date.
    c. The first time and date shall be assigned the override state that the point shall advance to when the time and date become current.
    d. The second time and date shall be assigned the state that the point shall return to when the time and date become current.
8. Copy command in database shall allow for like data to be copied and then edited for specific requirements, to reduce redundant data entry.

I. Operator Access Control:

1. Control operator access to system controls through three password-protected operator levels. System operators and managers with appropriate password clearances shall be able to change operator levels for operators.
2. Three successive attempts by an operator to execute functions beyond their defined level during a 24-hour period shall initiate a software tamper alarm.
3. A minimum of 32 passwords shall be available with the system software. System shall display the operator's name or initials in the console's first field. System shall print the operator's name or initials, action, date, and time on the system printer at login and logoff.
4. The password shall not be displayed or printed.
5. Each password shall be definable and assignable for the following:
    a. Selected commands to be usable.
    b. Access to system software.
    c. Access to application software.
    d. Individual zones that are to be accessed.
    e. Access to database.

J. Operator Commands:

1. Command Input: Plain-language words and acronyms shall allow operators to use the system without extensive training or data-processing backgrounds. System prompts shall be a word, a phrase, or an acronym.
2. Command inputs shall be acknowledged and processing shall start in not less than one second(s).
3. Tasks that are executed by operator's commands shall include the following:
    a. Acknowledge Alarms: Used to acknowledge that the operator has observed the alarm message.
    b. Place Zone in Access: Used to remotely disable intrusion-alarm circuits emanating from a specific zone. System shall be structured so that console operator cannot disable tamper circuits.
    c. Place Zone in Secure: Used to remotely activate intrusion-alarm circuits emanating from a specific zone.
    d. System Test: Allows the operator to initiate a system-wide operational test.
    e. Zone Test: Allows the operator to initiate an operational test for a specific zone.
    f. Print reports.
    g. Change Operator: Used for changing operators.
    h. Security Lighting Controls: Allows the operator to remotely turn on or turn off security lights.
    i. Display Graphics: Used to show any graphic displays implemented in the system. Graphic displays shall be completed within 20 seconds from time of operator command.
    j. Run system tests.
    k. Generate and format reports.
    l. Request help with the system operation.

1) Include in main menus.

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

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

4) Help shall be accessible outside the application program.

m. Entry-Control Commands:

1) Lock (secure) or unlock (open) each controlled entry and exit up to four times a day through time-zone programming.

2) Arm or disarm each monitored input up to four times a day through time-zone programming.

3) Enable or disable readers or keypads up to two times a day through time-zone programming.

4) Enable or disable cards or codes up to four times a day per entry point through access-level programming.

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

a. Command entered is incorrect or incomplete.

b. Operator is restricted from using that command.

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

d. Command addresses a point that does not exist.

e. Command is outside the system's capacity.

K. Alarms:

1. System Setup:

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

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

c. Sixty-character message field for each alarm.

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

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

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

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

2. Software Tamper:

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

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

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

d. Allow only acknowledgment of software tamper alarms.

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

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

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

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

7. Alarm Automation Interface: High-level interface to central-station alarm automation software systems. Allows input alarms to be passed to and handled by automation systems in the same manner as burglar alarms, using a TIA 232-F ASCII interface.

8. CCTV Alarm Interface: Allow commands to be sent to CCTV systems during alarms (or input change of state) through serial ports.

9. Camera Control: Provides operator ability to select and control cameras from graphic maps.

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

1. Displayed alarm data shall include type of alarm, location of alarm, and secondary alarm messages.

2. Printed alarm data shall include type of alarm, location of alarm, date and time (to nearest second) of occurrence, and operator responses.

3. Maps shall automatically display the alarm condition for each input assigned to that map if that option is selected for that input location.

4. Alarms initiate a status of "pending" and require the following two handling steps by operators:

a. First Operator Step: "Acknowledged." This action shall silence sounds associated with the alarm. The alarm remains in the system "Acknowledged" but "Un-Resolved."

b. Second Operator Step: Operators enter the resolution or operator comment, giving the disposition of the alarm event. The alarm shall then clear.

5. Each workstation shall display the total pending alarms and total unresolved alarms.

6. Each alarm point shall be programmable to disallow the resolution of alarms until the alarm point has returned to its normal state.

7. Alarms shall transmit to the central station in real time except for allowing connection time for dial-up locations.

8. Alarms shall be displayed and managed from a minimum of four different windows.

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

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

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

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

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

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

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

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

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

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

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

1. Color Code:

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

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

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

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

2. Graphics:

    a. Support 32,000 graphic display maps and allow import of maps from a minimum of 16 standard formats from another drawing or graphics program.

    b. Allow I/O to be placed on graphic maps by the drag-and-drop method.

    c. Operators shall be able to view the inputs, outputs, and the point's name by moving the mouse cursor over the point on the graphic map.

d. Inputs or outputs may be placed on multiple graphic maps. The operator shall be able to toggle to view graphic maps associated with I/Os.

e. Each graphic map shall have a display-order sequence number associated with it to provide a predetermined order when toggled to different views.

f. Camera icons shall have the ability to be placed on graphic maps that, when selected by an operator, will open a video window, display the camera associated with that icon, and provide pan-tilt-zoom control.

g. Input, output, or camera placed on a map shall allow the ability to arm or bypass an input, open or secure an output, or control the pan-tilt-zoom function of the selected camera.

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

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

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

1. Automatic Printing: Setup shall specify, modify, or inhibit the report to be generated; the time the initial report is to be generated; the time interval between reports; the end of the period; and the default printer.

2. Printing on Request: An operator may request a printout of any report.

3. Alarm Reports: Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm (such as door alarm, intrusion alarm, tamper alarm, etc.), the type of sensor, the location, the time, and the action taken.

4. Access and Secure Reports: Document zones placed in access, the time placed in access, and the time placed in secure mode.

5. Custom Reports: Reports tailored to exact requirements of who, what, when, and where. As an option, custom report formats may be stored for future printing.

6. Automatic History Reports: Named, saved, and scheduled for automatic generation.

7. Cardholder Reports: Include data, or selected parts of the data, as well as the ability to be sorted by name, card number, imprinted number, or by any of the user-defined fields.

8. Cardholder by Reader Reports: Based on who has access to a specific reader or group of readers by selecting the readers from a list.

9. Cardholder by Access-Level Reports: Display everyone that has been assigned to the specified access level.

10. Who Is "In" (Muster) Report:

a. Emergency Muster Report: One-click operation on toolbar launches report.

b. Cardholder Report. Contain a count of persons who are "In" at a selected Location and a detailed listing of name, date, and time of last use, sorted by the last reader used or by the group assignment.

11. Panel Labels Reports: Printout of control-panel field documentation including the actual location of equipment, programming parameters, and wiring identification. Maintain

system installation data within system database so that data is available on-site at all times.

12. Activity and Alarm On-Line Printing: Activity printers for use at workstations; prints all events, or alarms only.

13. History Reports: Custom reports that allow the operator to select any date, time, event type, device, output, input, operator, Location, name, or cardholder to be included or excluded from the report.

    a. Initially store history on the hard disk of the host PC.

    b. Permit viewing of the history on workstations or print history to any system printer.

    c. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.

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

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

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

14. Reports shall have the following four options:

    a. View on screen.

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

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

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

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

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

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

    c. Group, Location access levels.

    d. Start and stop code range.

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

    f. In, out, or either status.

    g. Codes with trace designation.

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

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

P. Anti-Passback:

1. System shall have global and local anti-passback features, selectable by Location. System shall support hard and soft anti-passback.

2. Hard Anti-Passback: Once a credential holder is granted access through a reader with one type of designation (IN or OUT), the credential holder may not pass through that type of reader designation until the credential holder passes through a reader of opposite designation.

3. Soft Anti-Passback: Should a violation of the proper IN or OUT sequence occur, access shall be granted, but a unique alarm shall be transmitted to the control station, reporting the credential holder and the door involved in the violation. A separate report may be run on this event.

4. Timed Anti-Passback: A controller capability that prevents an access code from being used twice at the same device (door) within a user-defined amount of time.

5. Provide four separate zones per Location that can operate without requiring interaction with the host PC (done at controller). Each reader shall be assignable to one or all four anti-passback zones. In addition, each anti-passback reader can be further designated as "Hard," "Soft," or "Timed" in each of the four anti-passback zones. The four anti-passback zones shall operate independently.

6. The anti-passback schemes shall be definable for each individual door.

7. The Master Access Level shall override anti-passback.

8. System shall have the ability to forgive (or reset) an individual credential holder or the entire credential-holder population anti-passback status to a neutral status.

Q. Visitor Assignment:

1. Provide for and allow an operator to be restricted to only working with visitors. The visitor badging subsystem shall assign credentials and enroll visitors. Allow only those access levels that have been designated as approved for visitors.

2. Provide an automated log of visitor name, time and doors accessed, and name of person contacted.

3. Allow a visitor designation to be assigned to a credential holder.

4. Security access system shall be able to restrict the access levels that may be assigned to credentials issued to visitors.

5. Allow operator to recall visitors' credential-holder file once a visitor is enrolled in the system.

6. The operator may designate any reader as one that deactivates the credential after use at that reader. The history log shall show the return of the credential.

7. System shall have the ability to use the visitor designation in searches and reports. Reports shall be able to print all or any visitor activity.

R. Time and Attendance:

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

2. Shall be provided to match IN and OUT reads and display cumulative time in for each day and cumulative time in for length designated in the report.

3. System software setup shall allow designation of selected access-control readers as time and attendance hardware to gather the clock-in and clock-out times of the users at these readers.

   a. Reports shall show in and out times for each day, total time in for each day, and a total time in for period specified by the user.

   b. Allow the operator to view and print the reports, or save the reports to a file.

c. Alphabetically sort reports on the person's last name, by Location or location group. Include all credential holders or optionally select individual credential holders for the report.

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

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

1. The enrollment station shall not have alarm response or acknowledgment functions.

2. Provide multiple, password-protected access levels. Database management and modification functions shall require a higher operator access level than personnel enrollment functions.

3. The program shall provide means to disable the enrollment station when it is unattended, to prevent unauthorized use.

4. The program shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations. In the case of personnel identity-verification subsystems, this shall include biometric data. Allow entry of personnel identifying information into the system database using menu selections and data fields. The data field names shall be customized during setup to suit user and site needs. Personnel identity-verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files.

5. Cardholder Data: Provide 99 user-defined fields. System shall have the ability to run searches and reports using any combination of these fields. Each user-defined field shall be configurable, using any combination of the following features:

a. MASK: Determines a specific format with which data must comply.

b. REQUIRED: Operator is required to enter data into field before saving.

c. UNIQUE: Data entered must be unique.

d. DEACTIVATE DATE: Data entered will be evaluated as an additional deactivate date for all cards assigned to this cardholder.

e. NAME ID: Data entered will be considered a unique ID for the cardholder.

6. Personnel Search Engine: A report generator with capabilities such as search by last name, first name, group, or any predetermined user-defined data field; by codes not used in definable number of days; by skills; or by seven other methods.

7. Multiple Deactivate Dates for Cards: User-defined fields to be configured as additional stop dates to deactivate any cards assigned to the cardholder.

8. Batch card printing.

9. Default card data can be programmed to speed data entry for sites where most card data are similar.

10. Enhanced ASCII File Import Utility: Allows the importing of cardholder data and images.

11. Card Expire Function: Allows readers to be configured to deactivate cards when a card is used at selected devices.

2.5 SYSTEM DATABASE

A. Database and database management software shall define and modify each point in database using operator commands. Definition shall include parameters and constraints associated with each system device.

B. Database Operations:

1. System data management shall be in a hierarchical menu-tree format, with navigation through expandable menu branches and manipulated with use of menus and icons in a main menu and system toolbar.

2. Navigational Aids:

a. Toolbar icons for add, delete, copy, print, capture image, activate, deactivate, and muster report.

b. Point and click feature to facilitate data manipulation.

c. Next and previous command buttons visible when editing database fields to facilitate navigation from one record to the next.

d. Copy command and copy tool in the toolbar to copy data from one record to create a new similar record.

3. Data entry shall be automatically checked for duplicate and illegal data and shall be verified for valid format.

4. System shall generate a memo or note field for each item that is stored in database, allowing the storing of information about any defining characteristics of the item. Memo field is used for noting the purpose for which the item was entered, reasons for changes that were made, and the like.

C. File Management:

1. File management shall include database backup and restoration system, allowing selection of storage media, including 3.5-inch floppy disk, Zip and Jaz drives, and designated network resources.

2. Operations shall be both manual and automatic modes. The number of automatic sequential backups before the oldest backup will be overwritten; FIFO mode shall be operator selectable.

3. Backup program shall provide manual operation from any PC on the LAN and shall operate while system remains operational.

D. Operator Passwords:

1. Support up to 32,00 individual system operators, each with a unique password.

2. One to eight alphanumeric characters.

3. Allow passwords to be case sensitive.

4. Passwords shall not be displayed when entered.

5. Passwords shall have unique and customizable password profile, and allow several operators to share a password profile. Include the following features in the password profile:

a. Predetermine the highest-level password profile for access to all functions and areas of program.

b. Allow or disallow operator access to any program operation, including the functions of View, Add, Edit, and Delete.

c. Restrict doors to which an operator can assign access.

6. Operators shall use a user name and password to log on to system. This user name and password shall be used to access database areas and programs as determined by the associated profile.

7. Make provision to allow the operator to log off without fully exiting program. User may be logged off but program will remain running while displaying the login window for the next operator.

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

1. Access authorization shall verify the facility code first, the card or card-and-PIN validation second, and the access level (time of day, day of week, date), anti-passback status, and number of uses last.

2. Use data-entry windows to view, edit, and issue access levels. Access-authorization entry-management system shall maintain and coordinate all access levels to prevent duplication or the incorrect creation of levels.

3. Allow assignment of multiple cards/codes to a cardholder.

4. Allow assignment of up to four access levels for each Location to a cardholder. Each access level may contain any combination of doors.

5. Each door may be assigned four time zones.

6. Access codes may be up to 11 digits in length.

7. Software shall allow the grouping of locations so cardholder data can be shared by all locations in the group.

8. Visitor Access: Issue a visitor badge for data tracking or photo ID purposes without assigning that person a card or code.

9. Cardholder Tracing: Allow for selection of cardholder for tracing. Make a special audible and visible annunciation at control station when a selected card or code is used at a designated code reader. Annunciation shall include an automatic display of the cardholder image.

10. Allow each cardholder to be given either an unlimited number of uses or a number from one to 9999 that regulates the number of times the card can be used before it is automatically deactivated.

11. Provide for cards and codes to be activated and deactivated manually or automatically by date. Provide for multiple deactivate dates to be preprogrammed.

F. Security Access Integration:

1. Photo ID badging and photo verification shall use the same database as the security access and may query data from cardholder, group, and other personal information to build a custom ID badge.

2. Automatic or manual image recall and manual access based on photo verification shall also be a means of access verification and entry.

3. System shall allow sorting of cardholders together by group or other characteristic for a fast and efficient method of reporting on, and enabling or disabling, cards or codes.

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

1. Provide the ability to store information about which conventional metal keys are issued and to whom, along with key construction information.

2. Reports shall be designed to list everyone who possesses a specified key.

H. Facility Codes: System shall accommodate up to 2048 facility codes per Location, with the option of allowing facility codes to work at all doors or only at particular doors.

I. Operator Comments:

1. With the press of one appropriate button on the toolbar, the user shall be permitted to enter operator comments into the history at any time.

2. Automatic prompting of operator comment shall occur before the resolution of each alarm.

3. Operator comments shall be recorded by time, date, and operator number.

4. Comments shall be sorted and viewed through reports and history.

5. The operator may enter comments in two ways; either or both may be used:

a. Manually entered through keyboard data entry (typed), up to 65,000 characters per each alarm.

b. Predefined and stored in database for retrieval on request.

6. System shall have a minimum of 999 predefined operator comments with up to 30 characters per comment.

J. Group:

1. Group names may be used to sort cardholders into groups that allow the operator to determine the tenant, vendor, contractor, department, division, or any other designation of a group to which the person belongs.

2. System software shall have the capacity to assign one of 32,000 group names to an access authorization.

3. Make provision in software to deactivate and reactivate all access authorizations assigned to a particular group.

4. Allow sorting of history reports and code list printouts by group name.

K. Time Zones:

1. Each zone consists of a start and stop time for seven days of the week and three holiday schedules. A time zone is assigned to inputs, outputs, or access levels to determine when an input shall automatically arm or disarm, when an output automatically opens or secures, or when access authorization assigned to an access level will be denied or granted.

2. Up to four time zones may be assigned to inputs and outputs to allow up to four arm or disarm periods per day or four lock or unlock periods per day; up to three holiday override schedules may be assigned to a time zone.

3. Data-entry window shall display a dynamically linked bar graph showing active and inactive times for each day and holiday, as start and stop times are entered or edited.

4. System shall have the capacity for [2048] <Insert number> time zones for each Location.

L. Holidays:

1. Three different holiday schedules may be assigned to a time zone. Holiday schedule consists of date in format MM/DD/YYYY and a description. When the holiday date matches the current date of the time zone, the holiday schedule replaces the time-zone schedule for that 24-hour period.

2. System shall have the capacity for [32,000] <Insert number> holidays.

3. Three separate holiday schedules may be applied to a time zone.

4. Holidays have an option to be designated as occurring on the designated date each year. These holidays remain in the system and will not be purged.

5. Holidays not designated to occur each year shall be automatically purged from the database after the date expires.

M. Access Levels:

1. System shall allow for the creation of up to [32,000] <Insert number> access levels.

2. One level shall be predefined as the Master Access Level. The Master Access Level shall work at all doors at all times and override any anti-passback.

3. System shall allow for access to be restricted to any area by reader and by time. Access levels shall determine when and where an Identifier is authorized.

4. System shall be able to create multiple door and time-zone combinations under the same access level so that an Identifier may be valid during different time periods at different readers even if the readers are on the same controller.

N. User-Defined Fields:

1. System shall provide a minimum of 99 user-defined fields, each with up to 50 characters, for specific information about each credential holder.

2. System shall accommodate a title for each field; field length shall be 20 characters.

3. A "Required" option may be applied to each user-defined field that, when selected, forces the operator to enter data in the user-defined field before the credential can be saved.

4. A "Unique" option may be applied to each user-defined field that, when selected, will not allow duplicate data from different credential holders to be entered.

5. Data format option may be assigned to each user-defined field that will require the data to be entered with certain character types in specific spots in the field entry window.

6. A user-defined field, if selected, will define the field as a deactivate date. The selection shall automatically cause the data to be formatted with the windows MM/DD/YYYY date format. The credential of the holder will be deactivated on that date.

7. A search function shall allow any one user-defined field or combination of user-defined fields to be searched to find the appropriate cardholder. The search function shall include a search for a character string.

8. System shall have the ability to print cardholders based on and organized by the user-defined fields.

O. Code Tracing:

1. System shall perform code tracing selectable by cardholder and by reader.

2. Any code may be designated as a "traced code" with no limit to how many codes can be traced.

3. Any reader may be designated as a "trace reader" with no limit to which or how many readers can be used for code tracing.

4. When a traced code is used at a trace reader, the access-granted message that usually appears on the monitor window of the central station shall be highlighted with a different color than regular messages. A short singular beep shall occur at the same time the highlighted message is displayed on the window.

5. The traced cardholder image (if image exists) shall appear on workstations when used at a trace reader.

2.6 SURGE AND TAMPER PROTECTION

A. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor-entry connection to components.

1. Minimum Protection for Power Connections 120 V and More: Auxiliary panel suppressors complying with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits."

2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Connections: Comply with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits." as recommended by manufacturer for type of line being protected.

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

2.7 CENTRAL-STATION HARDWARE

A. Central-Station Computer: Standard unmodified PC of modular design. The CPU word size shall be 32 bytes or larger; the CPU operating speed shall be at least 10 GHz.

1. Memory: 256 MB of usable installed memory, expandable to a minimum of 1024 MB without additional chassis or power supplies.

2. Power Supply: Minimum capacity of 250 W.

3. Real-Time Clock:

a. Accuracy: Plus or minus one minute per month.

b. Time-Keeping Format: 24-hour time format including seconds, minutes, hours, date, day, and month; resettable by software.

c. Clock shall function for one year without power.

d. Provide automatic time correction once every 24 hours by synchronizing clock with the Time Service Department of the U.S. Naval Observatory.

4. Serial Ports: Provide two TIA 232-F serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.

5. Parallel Port: An enhanced parallel port.

6. LAN Adapter Card: 10/100/1000 Mbps PCI bus, internal network interface card.

7. Sound Card: For playback and recording of digital WAV sound files that are associated with audible warning and alarm functions.

8. Color Monitor: Not less than 24 inches (430 mm), with a minimum resolution of 1280 by 1024 pixels, noninterlaced, and a maximum dot pitch of 0.28 mm. The video card shall support at least 256 colors at a resolution of 1280 by 1024 at a minimum refresh rate of 70 Hz.

9. Keyboard: With a minimum of 64 characters, standard ASCII character set based on ANSI INCITS 154.

10. Mouse: Standard, compatible with the installed software.

11. Special-function keyboard attachments or special-function keys to facilitate data input of the following operator tasks:

a. Help.

b. Alarm Acknowledge.

c. Place Zone in Access.

d. Place Zone in Secure.

e. System Test.

f. Print Reports.

g. Change Operator.

12. Disk storage shall include the following, each with appropriate controller:

a. Minimum 2 TB hard disk, maximum average access time of 10 ms.

b. DVD Drive.

c. PCMCIA slot with removable 500 MB media.

13. Magnetic Tape System: 4-mm cartridge magnetic tape system with minimum 20 GB formatted capacity per tape. Provide 10 tapes, each in a rigid cartridge with spring-loaded cover and operator-settable write-protect feature.

14. Audible Alarm: Manufacturer's standard.

15. DVD-ROM Drive:

a. Nominal storage capacity of 650 MB.

b. Data Transfer Rate: 1.2 Mbps.

c. Average Access Time: 150 ms.

d. Cache Memory: 256 KB.

e. Data Throughput: 1 MB/second, minimum.

16. Laser Alarm Printer:

a. Connected to the central station.

b. Minimum of 96 characters, standard ASCII character set based on ANSI INCITS 154, and with graphics capability and programmable top-of-form control.

c. Prints in color.

d. Adjustable sprockets for paper width up to 11 inches.

e. 80 columns per line, minimum speed of 200 characters per second.

f. Character Spacing: Selectable at 10, 12, or 17 characters per inch.

g. Paper: Sprocket-fed fan fold paper.

17. Interface: Bidirectional parallel, and universal serial bus.

18. LAN Adapter Card: 10/100/1000 Mbps internal network interface card.

B. UPS: Self-contained; complying with requirements in Division 26 Section "Static Uninterruptible Power Supply."

1. Size: Provide a minimum of six hours of operation of the central-station equipment, including two hours of alarm printer operation.

2. Batteries: Sealed, valve regulated, recombinant, lead calcium.

3. Accessories:

a. Transient voltage suppression.

b. Input-harmonics reduction.

c. Rectifier/charger.

d. Battery disconnect device.

e. Static bypass transfer switch.

f. Internal maintenance bypass/isolation switch.

g. External maintenance bypass/isolation switch.

h. Output isolation transformer.

i. Remote UPS monitoring.

j. Battery monitoring.

k. Remote battery monitoring.

2.8 STANDARD WORKSTATION HARDWARE

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

B. Workstation Computer: Standard unmodified PC of modular design. The CPU word size shall be 64 bytes or larger; the CPU operating speed shall be at least 66 MHz

1. Memory: 2000 MB of usable installed memory, expandable to a minimum of 8 GB without additional chassis or power supplies.

2. Power Supply: Minimum capacity of 400 W.

3. Real-Time Clock:

a. Accuracy: Plus or minus one minute per month.

b. Time-Keeping Format: 24-hour time format including seconds, minutes, hours, date, day, and month; resettable by software.

c. Provide automatic time correction once every 24 hours by synchronizing clock with the central station.

4. Serial Ports: Provide two TIA 232-F USB serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.

5. Parallel Port: An enhanced parallel port.

6. Sound Card: For playback and recording of digital WMP sound files that are associated with audible warning and alarm functions.

7. Color Monitor: Not less than 17 inches (430 mm), with a minimum resolution of 1280 by 1024 pixels, noninterlaced, and a maximum dot pitch of 0.28 mm. The video card shall support at least 256 colors at a resolution of 1280 by 1024 at a minimum refresh rate of 70 Hz.

8. Keyboard: With a minimum of 64 characters, standard ASCII character set based on ANSI INCITS 154.

9. Mouse: Standard, compatible with the installed software. Minimum resolution shall be 400 dpi.

10. Disk storage shall include the following, each with appropriate controller:

a. Minimum 2000 GB hard disk, maximum average access time of 10 ms.

b. DVD Drive

11. CD-ROM/CD-RW Drive:

a. Nominal Storage Capacity: 700 MB.

b. Data Transfer Rate: 3.6 Mbps.

c. Average Access Time: 150 ms.

d. Cache Memory:512 KB.

e. Data Throughput: 3.6 MB/second, minimum.

f. Read Speed: 48x.

g. Write Speed: 32x.

12. DVD/DVD-RW Drive:

a. Nominal Storage Capacity: 4.7> GB.

b. Data Transfer Rate: 3.6 Mbps.

c. Cache Memory: 512 KB.

d. Read Speed: 24x.

e. Write Speed: 6x.

13. Printer:

a. Connected to the central station and designated workstations.

b. Laser printer with minimum resolution of 600 dpi.

c. RAM: 8 MB, minimum.

d. Printing Speed: Minimum 12 pages per minute.

e. Paper Handling: Automatic sheet feeder with 250-sheet paper cassette and with automatic feed.

14. Interface: Bidirectional parallel, and universal serial bus.

15. LAN Adapter Card: 10/100/1000 Mbps internal network interface card.

2.9 CONTROLLER

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

B. Subject to compliance with requirements in this article, manufacturers may use multipurpose controller.

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

D. Alarm Annunciation Controller:

1. The controller shall automatically restore communication within 10 seconds after an interruption with the field device network, with dc line supervision on each of its alarm inputs.

a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.

b. Alarm-Line Supervision:

1) Supervise the alarm lines by monitoring each circuit for changes or disturbances in the signal, and for conditions as described in UL 1076 for

line security equipment by monitoring for abnormal open, grounded, or shorted conditions] using dc change measurements. System shall initiate an alarm in response to an abnormal current, which is a dc change of 5 percent or more for longer than 500 ms.

2) Transmit alarm-line-supervision alarm to the central station during the next interrogation cycle after the abnormal current condition.

E. Entry-Control Controller:

1. Function: Provide local entry-control functions including one- and two-way communications with access-control devices such as card readers, keypads, biometric personnel identity-verification devices, door strikes, magnetic latches, gate and door operators, and exit push buttons.

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

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

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

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

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

2. Inputs:

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

b. Database downloads and updates from the central station that include enrollment and privilege information.

3. Outputs:

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

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

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

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

4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.

5. Data Line Problems: For periods of loss of communication with the central station, or when data transmission is degraded and generating continuous checksum errors, the controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.

a. Store up to 1000 transactions during periods of communication loss between the controller and access-control devices for subsequent upload to the central station on restoration of communication.

6. Controller Power: NFPA 70, Class II power-supply transformer, with 12- or 24-V ac secondary, backup battery and charger.

a. Backup Battery: Valve-regulated, recombinant-sealed, lead-acid battery; spill proof. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.

b. Power Monitoring: Provide manual, dynamic battery-load test, initiated and monitored at the control center; with automatic disconnection of the controller when battery voltage drops below controller limits. Report by using local controller-mounted digital displays and by communicating status to central station. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:

1) Trouble Alarm: Normal power-off load assumed by battery.

2) Trouble Alarm: Low battery.

3) Alarm: Power off.

2.10 CARD READERS, CREDENTIAL CARDS, AND KEYPADS

A. Card-Reader Power: Powered from its associated controller, including its standby power source, and shall not dissipate more than 5 W.

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

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

1. Indoors, controlled environment.

2. Indoors, uncontrolled environment.

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

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

E. Stripe Swipe Readers: Bidirectional, reading cards swiped in both directions, powered by the controller. Reader shall be set up for ABA Track.

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

2. Readers for outdoors shall be in a polymeric plastic enclosure with all electronics potted in plastic. Rated for operation in ambient conditions of minus 40 to plus 160 deg F (minus 40 to plus 70 deg C) in a humidity range of 10 to 90 percent.

F. Wiegand Swipe Reader: Set up for 33-bit data cards. Comply with SIA AC-01.

G. Wiegand Key-Insert Reader: Set up for 33-bit data cards.

H. Insert Readers: Requiring the card to be inserted from the side, powered by the controller.

I. Touch-Plate and Proximity Readers:

1. Active-detection proximity card readers shall provide power to compatible credential cards through magnetic induction, and shall receive and decode a unique identification code number transmitted from the credential card.

2. Passive-detection proximity card readers shall use a swept-frequency, RF field generator to read the resonant frequencies of tuned circuits laminated into compatible credential cards. The resonant frequencies read shall constitute a unique identification code number.

3. The card reader shall read proximity cards in a range from direct contact to at least 6 inches (150 mm) from the reader.

J. Keypads:

1. Entry-control keypads shall use a unique combination of alphanumeric and other symbols as an Identifier.

2. Keypads shall contain an integral alphanumeric/special symbols keyboard with symbols arranged in ascending ASCII-code ordinal sequence.

3. Communication protocol shall be compatible with the local processor.

K. Keypad Display:

1. Keypads shall include a digital visual indicator and shall provide visible and audible status indications and user prompts.

2. Display shall indicate power on or off and whether user passage requests have been accepted or rejected.

3. Design of the keypad display or keypad enclosure shall limit viewing angles of the keypad as follows:

a. Maximum Horizontal Viewing Angle: Plus or minus 5 degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display.

b. Maximum Vertical Viewing Angle: Plus or minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.

L. Keypad Response Time:

1. The keypad shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 ms or less from the time the last alphanumeric symbol is entered until a response signal is generated.

M. Keypad Power:

1. The keypad shall be powered from the source as shown and shall not dissipate more than 150 W.

N. Keypad Mounting Method:

1. Keypads shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.

O. Keypad Duress Codes:

1. Keypads shall provide a means for users to indicate a duress situation by entering a special code.

P. Keypad and Wiegand-Swipe-Reader Combination: Designed to require an entry on the keypad before presenting the credential card.

1. Keypad: Allow the entry of four [numeric digits] [alphanumeric characters] that are associated with a specific credential. Keypads shall contain an integral alphanumeric/special symbol keyboard with symbols arranged in ascending ASCII-code

ordinal sequence. Keypad display or enclosure shall limit viewing angles of the keypad as follows:

a. Maximum Horizontal Viewing Angle: Plus or minus 5 degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display.

b. Maximum Vertical Viewing Angle: Plus or minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.

2. Wiegand Swipe Reader: Set up for 33-bit data cards to generate a unique card identification code. Comply with SIA AC-01.

Q. Communication Protocol: Compatible with local processor.

R. Touch-Plate and Contactless Card Reader: The reader shall have "flash" download capability to accommodate card format changes. The card reader shall have capability of transmitting data to security control panel and shall comply with ISO/IEC 7816.

S. Credential Card Modification: Entry-control cards shall be able to be modified by lamination direct print process during the enrollment process without reduction of readability. The design of the credential cards shall allow for the addition of at least one slot or hole to accommodate the attachment of a clip for affixing the credential card to the badge holder used at the site.

T. Card Size and Dimensional Stability: Credential cards shall be 2-1/8 by 3-3/8 inches (54 by 86 mm). The credential card material shall be dimensionally stable so that an undamaged card with deformations resulting from normal use shall be readable by the card reader.

U. Card Material: Abrasion resistant, nonflammable, nontoxic, and impervious to solar radiation and effects of ultraviolet light.

V. Card Construction:

1. Core and laminate or monolithic construction.

2. Lettering, logos, and other markings shall be hot stamped into the credential material or direct printed.

3. Furnish equipment for on-site assembly and lamination of credential cards.

2.11 ENROLLMENT CENTER

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. Applied Wireless Identifications Group, Inc.

2. Autostar Technology Pte Ltd.

3. Digital Monitoring Products.

4. IDenticard Systems.

5. ISONAS, Inc.

6. Ultra Electronics.

7. <Insert manufacturer's name>.

B. Equipment for enrolling personnel into, and removing personnel from, system database, using a dedicated workstation PC.

1. Include equipment to enroll selected biometric credentials.

C. Enrollment equipment shall support encoding of credential cards including cryptographic and other internal security checks as required for system.

1. Allow only authorized entry-control enrollment personnel to access the enrollment equipment using passwords.
2. Include enrollment-subsystem configuration controls and electronic diagnostic aids for subsystem setup and troubleshooting with the central station.
3. Enrollment-station records printer shall meet requirements of the report printer.

D. Entry-Control Enrollment Software:

1. Shall include database management functions for the system, and shall allow an operator to change and modify the data entered in the system as needed.
2. Software shall not have alarm response or acknowledgment functions as a programmable function.
3. Multiple, password-protected access levels shall be provided at the enrollment station.
4. Database management and modification functions shall require a higher operator-access level than personnel enrollment functions.
5. Software shall provide a means for disabling the enrollment station when it is unattended, to prevent unauthorized use.
6. Software shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations to include a credential unit in use at the installation.
7. In the case of personnel identity-verification subsystems, this data shall include biometric data.
8. Software shall allow entry of this data into the system database files through the use of simple menu selections and data fields. The data field names shall be customized to suit user and site needs.
9. Personnel identity-verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files.

E. Accessories:

1. Equipment rack or cabinet.
2. Equipment Rack: Comply with EIA/ECA-310-E.
3. Equipment, with the exception of the printers, shall be rack mounted in the console and equipment racks.

F. System Capacity: Number of badges shall be limited only by hard disk space. Badge templates and images shall be in color, supporting the maximum color capability of Microsoft Windows.

G. Badge Configuration:

1. Software for badge template creation shall include a template consisting of background and predetermined locations of photographs, text objects and data fields for text, and bar-code and biometric information. Include automatic sizing of data fields placed on a badge to compensate for names, which may otherwise be too large to fit in the area designated.
2. Allow different badge templates to be used for each department, tenant, or visitor.
3. As a setup option, templates shall be automatically selected for the badge, based on the group to which the credential holder is assigned. Allow the operator to override the

automatic template selection and use a template chosen by the operator for creating a badge.

4. Setup shall determine which graphics and credential-holder information will be displayed and where on the card it will be placed. All data in the security access system, such as name, code, group, access level, and any of the 99 user-defined fields, shall be selectable, with the ability to place them anywhere on the card.

5. System shall include an importing, filing, and recall system of stored images and shapes that can be placed on the badge.

6. Allow multiple images on the same badge, including, but not limited to, bar codes, digital photos, and signatures.

7. Support transparent backgrounds so that image is only surrounded by the intended background and not by its immediate background.

H. Photo Imaging: Integral to security access.

1. Import images from bitmap file formats, digital cameras, TWAIN cameras, or scanners. Allow image cropping and editing, WYSIWYG badge-building application, and badge print-preview and printing capabilities.

2. System shall support multiple images stored for each credential holder, including signatures, portrait views, and profile views.

I. Text Objects: Badge configuration shall provide for creation of custom text as an object, allowing font selection, typing, scaling, and formatting of the text object. Formatting options shall include changing font, font size, text flow, and text alignment; bending or curving the text object into a circle or semicircle; applying 3-D effects; and applying predefined effects such as tilt, extrusion, or beveling. Text shall be placed and optionally automatically centered within any region of the badge layout.

J. Badges and Credential Cards:

1. Badges are credential cards that do not contain data to be read by card readers.

2. Credential cards shall store uniquely coded data used by card readers as an Identifier.

a. Magnetic-Stripe Cards: Comply with ISO/IEC 7810, ISO/IEC 7811-1, ISO/IEC 7811-2, ISO/IEC 7811-6, and ISO/IEC 7811-7. Use single-layer magnetic tape material that is coated with a plastic, slick protective coat and affixed to the back of the credential card near the top.

b. Wiegand Wire-Effect Cards: Ferromagnetic wires laminated into the credential card using binary digits specified for Wiegand readers to generate a unique credential card identification code.

c. Proximity Cards: Use proximity detection without physical contact with the reader for proper operation.

3. Allow entry-control card to be modified by lamination or direct print process during the enrollment process for use as a picture and identification badge without reduction of readability. The design shall allow for the addition of at least one slot or hole to accommodate the attachment of a clip for affixing the credential card to the type of badge holder used at the site.

a. Card Size and Dimensional Stability: Standard size, 2-1/8 by 3-3/8 inches (54 by 86 mm); dimensionally stable so that an undamaged card with deformations resulting from normal use shall be readable by the card reader.

b. Card Material: Abrasion resistant, nonflammable, and nontoxic; and impervious to solar radiation and effects of ultraviolet light.

c. Card Construction: Core and laminate or monolithic construction. Lettering, logos, and other markings shall be hot stamped into the credential material or direct printed.

1) Furnish equipment for on-site assembly and lamination of credential cards.

d. Card Durability and Maintainability: Designed and constructed to yield a useful lifetime of at least five years or 5000 insertions or swipes, whichever results in a longer period of time. Allow credential cards to be cleaned by wiping with a sponge or cloth wetted with soap and water.

2.12 DOOR HARDWARE INTERFACE

A. Exit Device with Alarm: Operation of the exit device shall generate an alarm and annunciate a local alarm. Exit device and alarm contacts are specified in Division 08 Section "Door Hardware."

B. Exit Alarm: Operation of a monitored door shall generate an alarm. Exit devices and alarm contacts are specified in Division 08 Section "Door Hardware."

C. Electric Door Strikes: Use end-of-line resistors to provide power-line supervision. Signal switches shall transmit data to controller to indicate when the bolt is not engaged and the strike mechanism is unlocked, and they shall report a forced entry. Power and signal shall be from the controller. Electric strikes are specified in Division 08 Section "Door Hardware."

D. Electromagnetic Locks: End-of-line resistors shall provide power-line supervision. Lock status sensing signal shall positively indicate door is secure. Power and signal shall be from the controller. Electromagnetic locks are specified in Division 08 Section "Door Hardware."

2.13 FIELD-PROCESSING SOFTWARE

A. Operating System:

1. Local processors shall contain an operating system that controls and schedules that local processor's activities in real time.

2. Local processor shall maintain a point database in its memory that includes parameters, constraints, and the latest value or status of all points connected to that local processor.

3. Execution of local processor application programs shall utilize the data in memory resident files.

4. Operating system shall include a real-time clock function that maintains the seconds, minutes, hours, date, and month, including day of the week.

5. Local processor real-time clock shall be automatically synchronized with the central station at least once per day to plus or minus 10 seconds (the time synchronization shall be accomplished automatically, without operator action and without requiring system shutdown).

B. Startup Software:

1. Causes automatic commencement of operation without human intervention, including startup of all connected I/O functions.

2. Local processor restart program based on detection of power failure at the local processor shall be included in the local processor software.

3. Initiates operation of self-test diagnostic routines.

4. Upon failure of the local processor, if the database and application software are no longer resident, the local processor shall not restart and systems shall remain in the failure mode indicated until the necessary repairs are made.

5. If the database and application programs are resident, the local processor shall immediately resume operation.

C. Operating Mode:

1. Local processors shall control and monitor inputs and outputs as specified, independent of communications with the central station or designated workstations.

2. Alarms, status changes, and other data shall be transmitted to the central station or designated workstations when communications circuits are operable.

3. If communications are not available, each local processor shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the central station or designated workstations, shall be stored for later transmission to the central station or designated workstations.

4. Storage for the latest 4000 events shall be provided at local processors, as a minimum.

5. Local processors shall accept software downloaded from the central station.

6. Panel shall support flash ROM technology to accomplish firmware downloads from a central location.

D. Failure Mode: Upon failure for any reason, each local processor shall perform an orderly shutdown and force all local processor outputs to a predetermined (failure-mode) state, consistent with the failure modes shown and the associated control device.

E. Functions:

1. Monitoring of inputs.

2. Control of outputs.

3. Reporting of alarms automatically to the central station.

4. Reporting of sensor and output status to central station upon request.

5. Maintenance of real time, automatically updated by the central station at least once a day.

6. Communication with the central station.

7. Execution of local processor resident programs.

8. Diagnostics.

9. Download and upload data to and from the central station.

2.14 FIELD-PROCESSING HARDWARE

A. Alarm Annunciation Local Processor:

1. Respond to interrogations from the field device network, recognize and store alarm status inputs until they are transmitted to the central station, and change outputs based on commands received from the central station.

2. Local processor shall also automatically restore communication within 10 seconds after an interruption with the field device network and provide dc line supervision on each of its alarm inputs.

3. Local processor inputs shall monitor dry contacts for changes of state that reflect alarm conditions.

4. Local processor shall have at least eight alarm inputs which allow wiring contacts as normally open or normally closed for alarm conditions; and shall provide line supervision for each input by monitoring each input for abnormal open, grounded, or shorted conditions using dc current change measurements.

5. Local processor shall report line supervision alarms to the central station.

6. Alarms shall be reported for any condition that remains abnormal at an input for longer than 500 milliseconds.

7. Alarm condition shall be transmitted to the central computer during the next interrogation cycle.

8. Local processor outputs shall reflect the state of commands issued by the central station.

9. Outputs shall be a form C contact and shall include normally open and normally closed contacts.

10. Local processor shall have at least four command outputs.

11. Local processor shall be able to communicate with the central station via RS-485 or TCP/IP as a minimum.

B. Processor Power Supply:

1. Local processor and sensors shall be powered from an uninterruptible power source.

2. Uninterruptible power source shall provide eight hours of battery back-up power in the event of primary power failure and shall automatically fully recharge the batteries within 12 hours after primary power is restored.

3. If the facility is without an emergency generator, the uninterruptible power source shall provide 24 hours of battery backup power.

4. There shall be no equipment malfunctions or perturbations or loss of data during the switch from primary to battery power and vice versa.

5. Batteries shall be sealed, non-outgassing type.

6. Power supply shall be equipped with an indicator for ac input power and an indicator for dc output power.

7. Loss of primary power shall be reported to the central station as an alarm.

C. Auxiliary Equipment Power: A GFI service outlet shall be furnished inside the local processor's enclosure.

D. Entry-Control Local Processor:

1. Entry-control local processor shall respond to interrogations from the field device network, recognize and store alarm status inputs until they are transmitted to the central station, and change outputs based on commands received from the central station.

2. Local processor shall also automatically restore communication within 10 seconds after an interruption with the field device network and provide dc line supervision on each of its alarm inputs.

3. Entry-control local processor shall provide local entry-control functions including communicating with field devices such as card readers, keypads, biometric personnel identity-verification devices, door strikes, magnetic latches, gate and door operators, and exit push buttons.

4. Processor shall also accept data from entry-control field devices as well as database downloads and updates from the central station that include enrollment and privilege information.

5. Processor shall send indications of successful or failed attempts to use entry-control field devices and shall make comparisons of presented information with stored identification information.

6. Processor shall grant or deny entry by sending control signals to portal-control devices and mask intrusion-alarm annunciation from sensors stimulated by authorized entries.

7. Entry-control local processor shall use inputs from entry-control devices to change modes between access and secure.

8. Local processor shall maintain a date-time- and location-stamped record of each transaction and transmit transaction records to the central station.

9. Processor shall operate as a stand-alone portal controller using the downloaded database during periods of communication loss between the local processor and the central station.

10. Processor shall store a minimum of 4000 transactions during periods of communication loss between the local processor and the central station for subsequent upload to the central station upon restoration of communication.

11. Local processor inputs shall monitor dry contacts for changes of state that reflect alarm conditions.

12. Local processor shall have at least eight alarm inputs which allow wiring contacts as normally open or normally closed for alarm conditions; and shall also provide line supervision for each input by monitoring each input for abnormal open, grounded, or shorted conditions using dc current change measurements.

13. Local processor shall report line supervision alarms to the central station.

14. Alarms shall be reported for any condition that remains abnormal at an input for longer than 500 ms.

15. Alarm condition shall be transmitted to the central station during the next interrogation cycle.

16. Entry-control local processor shall include the necessary software drivers to communicate with entry-control field devices. Information generated by the entry-control field devices shall be accepted by the local processor and automatically processed to determine valid identification of the individual present at the portal.

17. Upon authentication of the credentials or information presented, the local processor shall automatically check privileges of the identified individual, allowing only those actions granted as privileges.

18. Privileges shall include, but are not limited to, time of day control, day of week control, group control, and visitor escort control. The local processor shall maintain a date-time- and location-stamped record of each transaction.

19. Transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

20. Local processor outputs shall reflect the state of commands issued by the central station.

21. Outputs shall be a form C contact and shall include normally open and normally closed contacts.

22. Local processor shall have at least four addressable outputs.

23. The entry-control local processor shall also provide control outputs to portal-control devices.

24. Local processor shall be able to communicate with the central station via RS-485 or TCP/IP as a minimum.

25. The system manufacturer shall provide strategies for downloading database information for panel configurations and cardholder data to minimize the required download time when using IP connectivity.

E. Alarm-System Interface:

1. TIA 232-F output shall be capable of transmitting alarms from other monitoring and alarm systems to central-station automation software.

2. Alternatively, alarms that are received by this access-control system are to be transferred to the alarm automation system as if they were sent through a digital alarm receiver.

a. System shall be able to transmit an individual message from any alarm input to a burglar-alarm automation monitoring system.

b. System shall be able to append to each message a predefined set of character strings as a prefix and a suffix.

2.15 CABLES

A. General Cable Requirements: Comply with requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security" and as recommended by system manufacturer for integration requirement.

B. PVC-Jacketed, TIA 232-F Cables:

1. Two pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, and individual aluminum-foil/polyester-tape shielded pairs with 100 percent shield coverage; PVC jacket.

2. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.

3. NFPA 70, Type CM.

4. Flame Resistance: UL 1581 vertical tray.

C. Plenum-Type, TIA 232-F Cables:

1. Two pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, and individual aluminum-foil/polyester-tape shielded pairs with 100 percent shield coverage; plastic jacket.

2. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.

3. NFPA 70, Type CMP.

4. Flame Resistance: NFPA 262 flame test.

D. PVC-Jacketed, TIA 485-A Cables: Two pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, PVC insulation, unshielded, PVC jacket, and NFPA 70, Type CMG.

E. Plenum-Type, TIA 485-A Cables:

1. Two pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and fluorinated-ethylene-propylene jacket.

2. NFPA 70, Type CMP.

3. Flame Resistance: NFPA 262 flame test.

F. Multiconductor, PVC, Reader and Wiegand Keypad Cables:

1. No. 22 AWG, paired and twisted multiple conductors, stranded (7x30) tinned copper conductors, semirigid PVC insulation, overall aluminum-foil/polyester-tape shield with 100

percent shield coverage, plus tinned copper braid shield with 65 percent shield coverage, and PVC jacket.

2. NFPA 70, Type CMG.

3. Flame Resistance: UL 1581 vertical tray.

4. For TIA 232-F applications.

G. Paired, PVC, Reader and Wiegand Keypad Cables:

1. Three pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, individual aluminum-foil/polyester-tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and PVC jacket.

2. NFPA 70, Type CM.

3. Flame Resistance: UL 1581 vertical tray.

H. Paired, PVC, Reader and Wiegand Keypad Cables:

1. Three pairs, twisted, No. 20 AWG, stranded (7x28) tinned copper conductors, polyethylene (polyolefin) insulation, individual aluminum-foil/polyester-tape shielded pairs each with No. 22 AWG, stranded (19x34) tinned copper drain wire, 100 percent shield coverage, and PVC jacket.

2. NFPA 70, Type CM.

3. Flame Resistance: UL 1581 vertical tray.

I. Paired, Plenum-Type, Reader and Wiegand Keypad Cables:

1. Three pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, individual aluminum-foil/polypropylene-tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and fluorinated-ethylene-propylene jacket.

2. NFPA 70, Type CMP.

3. Flame Resistance: NFPA 262 flame test.

J. Multiconductor, Plenum-Type, Reader and Wiegand Keypad Cables:

1. Six conductors, No. 20 AWG, stranded (7x28) tinned copper conductors, fluorinated-ethylene-propylene insulation, overall aluminum-foil/polyester-tape shield with 100 percent shield coverage plus tinned copper braid shield with 85 percent shield coverage, and fluorinated-ethylene-propylene jacket.

2. NFPA 70, Type CMP.

3. Flame Resistance: NFPA 262 flame test.

K. Paired, Lock Cables:

1. One pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.

2. NFPA 70, Type CMG.

3. Flame Resistance: UL 1581 vertical tray.

L. Paired, Plenum-Type, Lock Cables:

1. One pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.

2. NFPA 70, Type CMP.

3. Flame Resistance: NFPA 262 flame test.

M. Paired, Lock Cables:

1. One pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.

2. NFPA 70, Type CMG.

3. Flame Resistance: UL 1581 vertical tray.

N. Paired, Plenum-Type, Lock Cables:

1. One pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.

2. NFPA 70, Type CMP.

3. Flame Resistance: NFPA 262 flame test.

O. Paired, Input Cables:

1. One pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, overall aluminum-foil/polyester-tape shield with No. 22 AWG, stranded (7x30) tinned copper drain wire, 100 percent shield coverage, and PVC jacket.

2. NFPA 70, Type CMR.

3. Flame Resistance: UL 1666 riser flame test.

P. Paired, Plenum-Type, Input Cables:

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

2. NFPA 70, Type CMP.

3. Flame Resistance: NFPA 262 flame test.

Q. Paired, AC Transformer Cables:

1. One pair, twisted, No. 18 AWG, stranded (7x26) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.

2. NFPA 70, Type CMG.

R. Paired, Plenum-Type, AC Transformer Cables:

1. One pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.

2. NFPA 70, Type CMP.

3. Flame Resistance: NFPA 262 flame test.

S. LAN Cabling:

1. Comply with requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."

2. NFPA 262.

2.16 TRANSFORMERS

A. NFPA 70, Class II control transformers, NRTL listed. Transformers for security access-control system shall not be shared with any other system.

PART 3 - EXECUTION

3.1 EXAMINATION

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

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

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

3.2 PREPARATION

A. Comply with recommendations in SIA CP-01.

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

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

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

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

3.3 CABLING

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

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

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.

D. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters and except in accessible ceiling spaces and in gypsum board partitions where unenclosed wiring method may be used. Use NRTL-listed plenum cable in environmental airspaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces.

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

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

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

3.4 CABLE APPLICATION

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

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

C. TIA 232-F Cabling: Install at a maximum distance of 50 ft. (15 m).

D. TIA 485-A Cabling: Install at a maximum distance of 4000 ft. (1220 m).

E. Card Readers and Keypads:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.

2. Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from controller to the reader is 250 ft. (75 m), and install No. 20 AWG wire if maximum distance is 500 ft. (150 m).

3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the controller.

4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.

F. Install minimum No. 16 AWG cable from controller to electrically powered locks

G. Install minimum No. 18 AWG ac power wire from transformer to controller.

3.5 GROUNDING

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

B. Comply with IEEE 1100, "Recommended Practice for Power and Grounding Electronic Equipment."

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

D. Bond shields and drain conductors to ground at only one point in each circuit.

E. Signal Ground:

1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.

2. Bus: Mount on wall of main equipment room with standoff insulators.

3. Backbone Cable: Extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

3.6 INSTALLATION

A. Push Buttons: Where multiple push buttons are housed within a single switch enclosure, they shall be stacked vertically with each push-button switch labeled with 1/4-inch- (6.4-mm-) high text and symbols as required. Push-button switches shall be connected to the controller associated with the portal to which they are applied, and shall operate the appropriate electric strike, electric bolt, or other facility release device.

B. Install card readers, keypads, push buttons, and biometric readers.

3.7 IDENTIFICATION

A. In addition to requirements in this article, comply with applicable requirements in Division 26 Section "Identification for Electrical Systems" and with TIA/EIA 606-A.

B. Using software specified in "Cable and Asset Management Software" Article, develop cable administration drawings for system identification, testing, and management. Use unique, alphanumeric designation for each cable, and label cable and jacks, connectors, and terminals to which it connects with the same designation. Use logical and systematic designations for facility's architectural arrangement.

C. Label each terminal strip and screw terminal in each cabinet, rack, or panel.

1. All wiring conductors connected to terminal strips shall be individually numbered, and each cable or wiring group being extended from a panel or cabinet to a building-mounted device shall be identified with the name and number of the particular device as shown.

2. Each wire connected to building-mounted devices is not required to be numbered at the device if the color of the wire is consistent with the associated wire connected and numbered within the panel or cabinet.

D. At completion, cable and asset management software shall reflect as-built conditions.

3.8 SYSTEM SOFTWARE AND HARDWARE

A. Develop, install, and test software and hardware, and perform database tests for the complete and proper operation of systems involved. Assign software license to Owner.

3.9 FIELD QUALITY CONTROL

A. Perform tests and inspections.

1. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.

B. Tests and Inspections:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA 568-B.1, "Commercial Building Telecommunications Cabling Standards - Part 1: General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA 568-B.1.

2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power-supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall

be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.

3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

C. Devices and circuits will be considered defective if they do not pass tests and inspections.

D. Prepare test and inspection reports.

3.10 STARTUP SERVICE

A. Engage a factory-authorized service representative to supervise and assist with startup service.

1. Complete installation and startup checks according to approved procedures that were developed in "Preparation" Article and with manufacturer's written instructions.

2. Enroll and prepare badges and access cards for Owner's operators, management, and security personnel.

3.11 PROTECTION

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

3.12 DEMONSTRATION

A. [Engage a factory-authorized service representative to train] [Train] Owner's maintenance personnel to adjust, operate, and maintain security access system. See Division 01 Section "Demonstration and Training."

B. Develop separate training modules for the following:

1. Computer system administration personnel to manage and repair the LAN and databases and to update and maintain software.

2. Operators who prepare and input credentials to man the control station and workstations and to enroll personnel.

3. Security personnel.

4. Hardware maintenance personnel.

5. Corporate management.

***** END OF SECTION *****

THIS PAGE IS INTENTIONALLY BLANK

SECTION 28 16 00

INTRUSION DETECTION

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. Section Includes:

1. Intrusion detection with communication links to perform monitoring, alarm, and control functions.

2. Integration of other electronic and electrical systems and equipment.

1.3 DEFINITIONS

A. CCTV: Closed-circuit television.

B. PIR: Passive infrared.

C. RFI: Radio-frequency interference.

D. Control Unit: System component that monitors inputs and controls outputs through various circuits.

E. Master Control Unit: System component that accepts inputs from other control units and may also perform control-unit functions. The unit has limited capacity for the number of protected zones and is installed at an unattended location or at a location where it is not the attendant's primary function to monitor the security system.

F. Monitoring Station: Facility that receives signals and has personnel in attendance at all times to respond to signals. A central station is a monitoring station that is listed.

G. Protected Zone: A protected premises or an area within a protected premise that is provided with means to prevent an unwanted event.

H. Standard Intruder: A person who weighs 100 lb (45 kg) or less and whose height is 60 inches (1525 mm) or less; dressed in a long-sleeved shirt, slacks, and shoes.

I. Standard-Intruder Movement: Any movement, such as walking, running, crawling, rolling, or jumping, of a "standard intruder" in a protected zone.

J. Systems Integration: The bringing together of components of several systems containing interacting components to achieve indicated functional operation of combined systems.

K. Zone. A defined area within a protected premise. It is a space or area for which an intrusion must be detected and uniquely identified. The sensor or group of sensors must then be assigned to perform the detection, and any interface equipment between sensors and communication must link to master control unit.

1.4 SUBMITTALS

A. Product Data: Components for sensing, detecting, systems integration, and control, including dimensions and data on features, performance, electrical characteristics, ratings, and finishes.

B. Shop Drawings: Detail assemblies of standard components that are custom assembled for specific application on this Project.

1. Functional Block Diagram: Show single-line interconnections between components including interconnections between components specified in this Section and those furnished under other Sections. Indicate methods used to achieve systems integration. Indicate control, signal, and data communication paths and identify programmable logic controllers, networks and control interface devices and media to be used. Describe characteristics of network and other data communication lines.
    a. Indicate methods used to achieve systems integration.
    b. Indicate control, signal, and data communication paths and identify PLCs, networks, control interface devices, and media to be used.
    c. Describe characteristics of network and other data communication lines.
    d. Describe methods used to protect against power outages and transient voltages including types and ratings of isolation and surge suppression devices used in data, communication, signal, control, and ac and dc power circuits.
2. Raceway Riser Diagrams: Detail raceway runs required for intrusion detection and for systems integration. Include designation of devices connected by raceway, raceway type and size, and type and size of wire and cable fill for each raceway run.
3. UPS: Sizing calculations.
4. Site and Floor Plans: Indicate final outlet and device locations, routing of raceways, and cables inside and outside the building. Include room layout for master control-unit console, terminal cabinet, racks, and UPS.
5. Master Control-Unit Console Layout: Show required artwork and device identification.
6. Device Address List: Coordinate with final system programming.
7. System Wiring Diagrams: Include system diagrams unique to Project. Show connections for all devices, components, and auxiliary equipment. Include diagrams for equipment and for system with all terminals and interconnections identified.
8. Details of surge-protection devices and their installation.
9. Sensor detection patterns and adjustment ranges.

C. Equipment and System Operation Description: Include method of operation and supervision of each component and each type of circuit. Show sequence of operations for manually and automatically initiated system or equipment inputs. Description must cover this specific Project; manufacturer's standard descriptions for generic systems are unacceptable.

D. Samples for Initial Selection: For units with factory-applied color finishes.

E. Samples for Verification: For each type of exposed finish required.

F. Qualification Data: For Installer and testing agency.

G. Field quality-control reports.

H. Operation and Maintenance Data: For intrusion detection system to include in emergency, operation, and maintenance manuals. In addition to items specified in Division 01 Section "Operation and Maintenance Data," include the following:
    1. Data for each type of product, including features and operating sequences, both automatic and manual.
    2. Master control-unit hardware and software data.

I. Warranty: Sample of special warranty.

J. Other Information Submittals:

1. Test Plan and Schedule: Test plan defining all tests required to ensure that system meets technical, operational, and performance specifications.

2. Examination reports documenting inspections of substrates, areas, and conditions.

3. Anchor inspection reports documenting inspections of built-in and cast-in anchors.

1.5 QUALITY ASSURANCE

A. Installer Qualifications:

1. An employer of workers, at least one of whom is a technician certified by the National Burglar & Fire Alarm Association.

2. Manufacturer's authorized representative who is trained and approved for installation of units required for this Project.

B. Intrusion Detection Systems Integrator Qualifications: An experienced intrusion detection equipment supplier and Installer who has completed systems integration work for installations similar in material, design, and extent to that indicated for this Project, whose work has resulted in construction with a record of successful in-service performance.

C. Testing Agency Qualifications: Member company of NETA or an NRTL.

1. Testing Agency's Field Supervisor: Currently certified by NETA to supervise on-site testing.

D. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

E. Control Units, Devices, and Communications with Monitoring Station: Listed and labeled by a qualified testing agency for compliance with SIA CP-01.

F. FM Global Compliance: FM-Approved and -labeled intrusion detection devices and equipment.

G. Comply with NFPA 70.

1.6 PROJECT CONDITIONS

A. Environmental Conditions: Capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:

1. Altitude: Sea level to 4000 feet (1220 m).

2. Master Control Unit: Rated for continuous operation in an ambient of 60 to 85 deg F (16 to 29 deg C) and a relative humidity of 20 to 80 percent, noncondensing.

3. Interior, Controlled Environment: System components, except master control unit, installed in air-conditioned interior environments shall be rated for continuous operation in ambient of 36 to 122 deg F (2 to 50 deg C) dry bulb and 20 to 90 percent relative humidity, noncondensing.

4. Interior, Uncontrolled Environment: System components installed in non-air-conditioned interior environments shall be rated for continuous operation in ambient of 0 to 122 deg F (minus 18 to plus 50 deg C) dry bulb and 20 to 90 percent relative humidity, noncondensing.

1.7 WARRANTY

A. Special Warranty: Manufacturer's standard form in which manufacturer and Installer agree to repair or replace components of intrusion detection devices and equipment that fail in materials or workmanship within specified warranty period.

1. Warranty Period: Two years from date of Substantial Completion.

1.8 EXTRA MATERIALS

A. Furnish extra materials that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.

1. Intrusion Detection Devices: Furnish quantity equal to five percent of the number of units of each type installed, but no fewer than one of each type.

2. Fuses: Three of each kind and size.

3. Tool Kit: Provide six sets of tools for use with security fasteners, each packaged in a compartmented kit configured for easy handling and storage.

4. Security Fasteners: Furnish no fewer than 1 box for every 50 boxes or fraction thereof, of each type and size of security fastener installed.

PART 2 - PRODUCTS

2.1 FUNCTIONAL DESCRIPTION OF SYSTEM

A. Description: Multiplexed, modular, microprocessor-based controls, intrusion sensors and detection devices, and communication links to perform monitoring, alarm, and control functions.

B. Supervision: System components shall be continuously monitored for normal, alarm, supervisory, and trouble conditions. Indicate deviations from normal conditions at any location in system. Indication includes identification of device or circuit in which deviation has occurred and whether deviation is an alarm or malfunction.

1. Alarm Signal: Display at master control unit and actuate audible and visual alarm devices.

2. Trouble Condition Signal: Distinct from other signals, indicating that system is not fully functional. Trouble signal shall indicate system problems such as battery failure, open or shorted transmission line conductors, or control-unit failure.

3. Supervisory Condition Signal: Distinct from other signals, indicating an abnormal condition as specified for the particular device or control unit.

C. System Control: Master control unit shall directly monitor intrusion detection units and connecting wiring.

D. System Control: Master control unit shall directly monitor intrusion detection devices**,** perimeter detection units, control units associated with perimeter detection units, and connecting wiring in a multiplexed distributed control system or as part of a network.

E. System shall automatically reboot program without error or loss of status or alarm data after any system disturbance.

F. Operator Commands:

1. Help with System Operation: Display all commands available to operator. Help command, followed by a specific command, shall produce a short explanation of the purpose, use, and system reaction to that command.

2. Acknowledge Alarm: To indicate that alarm message has been observed by operator.

3. Place Protected Zone in Access: Disable all intrusion-alarm circuits of a specific protected zone. Tamper circuits may not be disabled by operator.

4. Place Protected Zone in Secure: Activate all intrusion-alarm circuits of a protected zone.

5. Protected Zone Test: Initiate operational test of a specific protected zone.

6. System Test: Initiate system-wide operational test.

7. Print reports.

G. Timed Control at Master Control Unit: Allow automatically timed "secure" and "access" functions of selected protected zones.

H. Automatic Control of Related Systems: Alarm or supervisory signals from certain intrusion detection devices control the following functions in related systems:

1. Switch selected lights.

2. Shift elevator control to a different mode.

3. Open a signal path between certain intercommunication stations.

4. Shift sound system to "listening mode" and open a signal path to certain system speakers.

5. Switch signal to selected monitor from CCTV camera in vicinity of sensor signaling an alarm.

I. Printed Record of Events: Print a record of alarm, supervisory, and trouble events on system printer. Sort and report by protected zone, device, and function. When master control unit receives a signal, print a report of alarm, supervisory, or trouble condition. Report type of signal (alarm, supervisory, or trouble), protected zone description, date, and time of occurrence. Differentiate alarm signals from other indications. When system is reset, report reset event with the same information concerning device, location, date, and time. Commands shall initiate the reporting of a list of current alarm, supervisory, and trouble conditions in system or a log of past events.

J. Response Time: Two seconds between actuation of any alarm and its indication at master control unit.

K. Circuit Supervision: Supervise all signal and data transmission lines, links with other systems, and sensors from master control unit. Indicate circuit and detection device faults with both protected zone and trouble signals, sound a distinctive audible tone, and illuminate an LED. Maximum permissible elapsed time between occurrence of a trouble condition and indication at master control unit is 20 seconds. Initiate an alarm in response to opening, closing, shorting, or grounding of a signal or data transmission line.

L. Programmed Secure-Access Control: System shall be programmable to automatically change status of various combinations of protected zones between secure and access conditions at scheduled times. Status changes may be preset for repetitive, daily, and weekly; specially scheduled operations may be preset up to a year in advance. Manual secure-access control stations shall override programmed settings.

M. Manual Secure-Access Control: Coded entries at manual stations shall change status of associated protected zone between secure and access conditions.

2.2 SYSTEM COMPONENT REQUIREMENTS

A. Compatibility: Detection devices and their communication features, connecting wiring, and master control unit shall be selected and configured with accessories for full compatibility with the following equipment:

1. Access control system specified in Division 28 Section "Access Control."

2. Video surveillance system specified in Division 28 Section "Video Surveillance."

B. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor entry connection to components.

1. Minimum Protection for Power Lines 120 V and More: Auxiliary panel suppressors complying with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits."

2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Lines: Listed and labeled by a qualified testing agency for compliance with NFPA 731.

C. Intrusion Detection Units: Listed and labeled by a qualified testing agency for compliance with UL 639.

D. Interference Protection: Components shall be unaffected by radiated RFI and electrical induction of 15 V/m over a frequency range of 10 to 10,000 MHz and conducted interference signals up to 0.25-V rms injected into power supply lines at 10 to 10,000 MHz.

E. Tamper Protection: Tamper switches on detection devices, control units, annunciators, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled and when entering conductors are cut or disconnected. Master control-unit alarm display shall identify tamper alarms and indicate locations.

F. Self-Testing Devices: Automatically test themselves periodically, but not less than once per hour, to verify normal device functioning and alarm initiation capability. Devices transmit test failure to master control unit.

G. Antimasking Devices: Automatically check operation continuously or at intervals of a minute or less, and use signal-processing logic to detect blocking, masking, jamming, tampering, or other operational dysfunction. Devices transmit detection of operational dysfunction to master control unit as an alarm signal.

H. Addressable Devices: Transmitter and receivers shall communicate unique device identification and status reports to master control unit.

I. Remote-Controlled Devices: Individually and remotely adjustable for sensitivity and individually monitored at master control unit for calibration, sensitivity, and alarm condition.

2.3 ENCLOSURES

A. Interior Sensors: Enclosures that protect against dust, falling dirt, and dripping noncorrosive liquids.

B. Interior Electronics: NEMA 250, Type 12.

C. Screw Covers: Where enclosures are readily accessible, secure with security fasteners of type appropriate for enclosure.

2.4 SECURE AND ACCESS DEVICES

A. Basis-of-Design Product: Subject to compliance with requirements, provide Product by one of the following:

1. Bosch Security Systems, Inc.

2. Corby Industries, Inc.

3. Crow Electronic Engineering, Inc.

4. DAQ Electronics, Inc.

5. Digital Security Controls Ltd.; a business unit of Tyco Safety Products.

6. Edwards Signaling & Security Systems; part of GE Security.

7. Honeywell International Inc.; Honeywell Security.

8. Visonic Inc.

B. Keypad and Display Module: Arranged for entering and executing commands for system-status changes and for displaying system-status and command-related data.

C. Key-Operated Switch: Change protected zone between secure and access conditions.

2.5 DOOR AND WINDOW SWITCHES

A. Basis-of-Design Product: Subject to compliance with requirements, provide product by one of the following:

1. Aleph America Corporation.
2. General Electric Company; GE Security, Inc.
3. George Risk Industries.
4. Honeywell International Inc.; Honeywell Security.
5. Honeywell International Inc.; Honeywell Video Systems.
6. Optex Inc.
7. Potter Electric Signal, LLC.

B. Description: Balanced-magnetic switch, complying with UL 634, installed on frame with integral overcurrent device to limit current to 80 percent of switch capacity. Bias magnet and minimum of three encapsulated reed switches shall resist compromise from introduction of foreign magnetic fields.

C. Flush-Mounted Switches: Unobtrusive and flush with surface of door and window frame.

D. Overhead Door Switch: Balanced-magnetic type, listed for outdoor locations, and having door-mounted magnet and floor-mounted switch unit.

E. Remote Test: Simulate movement of actuating magnet from master control unit.

2.6 PIR SENSORS

A. Basis-of-Design Product: Subject to compliance with requirements, provide product by one of the following:

1. Aleph America Corporation.
2. Bosch Security Systems, Inc.
3. Crow Electronic Engineering, Inc.
4. Digital Security Controls Ltd.; a business unit of Tyco Safety Products.
5. General Electric Company; GE Security, Inc.
6. Honeywell International Inc.; Honeywell Security.
7. Visonic Inc.

B. Listed and labeled by a qualified testing agency for compliance with SIA PIR-01.

C. Description: Sensors detect intrusion by monitoring infrared wavelengths emitted from a human body within their protected zone and by being insensitive to general thermal variations.

1. Wall-Mounted Unit Maximum Detection Range: 125 percent of indicated distance for individual units and not less than 50 feet (15 m). Provide adjustable coverage pattern as indicated.
2. Ceiling-Mounted Unit Spot-Detection Pattern: Full 360-degree conical.
3. Ceiling-Mounted Unit Pattern Size: 84-inch (2135-mm) diameter at floor level for units mounted 96 inches (2440 mm) above floor; 18-foot (5.5-m) diameter at floor level for units mounted 25 feet (7.6 m) above floor.

D. Device Performance:

1. Sensitivity: Adjustable pattern coverage to detect a change in temperature of 2 deg F (1 deg C) or less, and standard-intruder movement within sensor's detection patterns at any speed between 0.3 to 7.5 fps (0.09 to 2.3 m/s) across two adjacent segments of detector's field of view.

2. Test Indicator: LED test indicator that is not visible during normal operation. When visible, indicator shall light when sensor detects an intruder. Locate test enabling switch under sensor housing cover.

3. Remote Test: When initiated by master control unit, start a test sequence for each detector element that simulates standard-intruder movement within sensor's detection patterns, causing an alarm.

2.7 MICROWAVE INTRUSION DETECTORS (INTERIOR)

A. Basis-of-Design Product: Subject to compliance with requirements, provide product by one of the following:

1. Bosch Security Systems, Inc.

2. Crow Electronic Engineering, Inc.

3. Digital Security Controls Ltd.; a business unit of Tyco Safety Products.

4. General Electric Company; GE Security, Inc.

5. Visonic Inc.

B. Device Performance: Microwave transmitter establishes an electromagnetic field in an adjustable detection pattern and detects intrusion by monitoring changes in that pattern.

1. Sensitivity: Adjustable, able to detect standard-intruder movement within sensor's detection pattern at any speed between 0.3 to 7.5 fps (0.09 to 2.3 m/s). Sensor sensitivity adjustments shall be accessible only when sensor housing is removed, and sensors shall comply with 47 CFR 15.

2. Activation Indicator: LED indicator shall not be visible during normal operation. Indicator shall light when sensor detects a standard intruder. Locate test-enabling switch under sensor housing cover.

3. Remote Test: When initiated by master control unit, start a test sequence for each detector element that simulates standard-intruder movement within sensor's detection patterns, causing an alarm.

2.8 MICROWAVE-PIR DUAL-TECHNOLOGY SENSORS

A. Basis-of-Design Product: Subject to compliance with requirements, provide product by one of the following:

1. Aleph America Corporation.

2. General Electric Company; GE Security, Inc.

3. Honeywell International Inc.; Honeywell Security.

4. Visonic Inc.

B. Description: Single unit combining a sensor that detects changes in microwave signals and a PIR sensor that detects changes in ambient level of infrared emissions caused by standard-intruder movement within detection pattern.

C. Listed and labeled by a qualified testing agency for compliance with SIA PIR-01.

D. Device Performance: An alarm is transmitted when either sensor detects a standard intruder within a period of three to eight seconds from when the other sensor detects a standard intruder.

1. Minimum Detection Pattern: A room 20 by 30 feet (6 by 9 m).

2. PIR Sensor Sensitivity: Adjustable pattern coverage to detect a change in temperature of 2 deg F (1 deg C) or less, and standard-intruder movement within sensor's detection patterns at any speed between 0.3 to 7.5 fps (0.09 to 2.3 m/s) across two adjacent segments of detector's field of view.

3. Microwave Sensor Sensitivity: Adjustable, able to detect standard-intruder movement within sensor's detection pattern at any speed between 0.3 to 7.5 fps (0.09 to 2.3 m/s). Sensor sensitivity adjustments shall be accessible only when sensor housing is removed, and sensors shall comply with 47 CFR 15.

4. Activation Indicator: LED indicator shall not be visible during normal operation. Indicator shall light when sensor detects a standard intruder. Locate test enabling switch under sensor housing cover.

5. Remote Test: When initiated by master control unit, start a test sequence for each detector element that simulates standard-intruder movement within sensor's detection patterns, causing an alarm.

2.9 MASTER CONTROL UNIT

A. Basis-of-Design Product: Subject to compliance with requirements, provide product by one of the following:

1. Bosch Security Systems, Inc.

2. DAQ Electronics, Inc.

3. Digital Security Controls, Inc.; a business unit of Tyco Safety Products.

4. General Electric Company; GE Security, Inc.

5. Honeywell International Inc.; Honeywell Security.

6. Honeywell International Inc.; Honeywell Video Systems.

7. Visonic Inc.

B. Description: Supervise sensors and detection subsystems and their connecting communication links, status control (secure or access) of sensors and detector subsystems, activation of alarms and supervisory and trouble signals, and other indicated functions.

1. System software and programs shall be held in flash electrically erasable programmable read-only memory (EEPROM), retaining the information through failure of primary and secondary power supplies.

2. Include a real-time clock for time annotation of events on the event recorder and printer.

3. Addressable initiation devices that communicate device identity and status.

4. Control circuits for operation of mechanical equipment in response to an alarm.

C. Construction: Freestanding equipment rack, modular, with separate and independent alarm and supervisory system modules. Alarm-initiating protected zone boards shall be plug-in cards. Arrangements that require removal of field wiring for module replacement are unacceptable.

D. Comply with UL 609.

E. Console Controls and Displays: Arranged for interface between human operator at master control unit and addressable system components including annunciation and supervision.

Display alarm, supervisory, and component status messages and the programming and control menu.

1. Annunciator and Display: LCD, three line(s) of 80 characters, minimum.
2. Keypad: Arranged to permit entry and execution of programming, display, and control commands.
3. Control-Unit Network: Automatic communication of alarm, status changes, commands, and other communications required for system operation. Communication shall return to normal after partial or total network interruption such as power loss or transient event. Total or partial signaling network failures shall identify the failure and record the failure at the annunciator display and at the system printer.
4. Field Device Network: Communicate between the control unit and field devices of the system. Communications shall consist of alarm, network status, and status and control of field-mounted processors. Each field-mounted device shall be interrogated during each interrogation cycle.
5. Operator Controls: Manual switches and push-to-test buttons that do not require a key to operate. Prevent resetting of alarm, supervisory, or trouble signals while alarm or trouble condition persists. Include the following:
    a. Acknowledge alarm.
    b. Silence alarm.
    c. System reset.
    d. LED test.
6. Timing Unit: Solid state, programmable, 365 days.
7. Confirmation: Relays, contactors, and other control devices shall have auxiliary contacts that provide confirmation signals to system for their on or off status. Software shall interpret such signals, display equipment status, and initiate failure signals.
8. Alarm Indication: Audible signal sounds and an LED lights at master control unit identifying the addressable detector originating the alarm. Annunciator panel displays a common alarm light and sounds an audible tone.
9. Alarm Indication: Audible signal sounds and a plain-language identification of the addressable detector originating the alarm appears on LED display at master control unit. Annunciator panel displays a common alarm light and sounds an audible tone.
10. Alarm Indication: Audible signal sounds and a plain-language identification of the addressable detector originating the alarm appears on LED display at master control unit. Annunciator panel alarm light and audible tone identify protected zone signaling an alarm.
11. Alarm activation sounds a siren and strobe.

F. Protected Zones: Quantity of alarm and supervisory zones as indicated, with capacity for expanding number of protected zones by a minimum of 25 percent.

G. Power Supply Circuits: Master control units shall provide power for remote power-consuming detection devices. Circuit capacity shall be adequate for at least a 25 percent increase in load.

H. UPS: Comply with Division 26 Section "Static Uninterruptible Power Supply." UPS shall be sized to provide a minimum of six hours of master control-unit operation.

I. Cabinet: Lockable, steel enclosure arranged so operations required for testing, normal operation, and maintenance are performed from front of enclosure. If more than a single cabinet is required to form a complete control unit, provide exactly matching modular

enclosures. Accommodate all components and allow ample gutter space for field wiring. Identify each enclosure by an engraved, laminated, phenolic-resin nameplate. Lettering on enclosure nameplate shall not be less than 1 inch (25 mm) high. Identify, with permanent labels, individual components and modules within cabinets.

J. Transmission to Monitoring Station: A communications device to automatically transmit alarm, supervisory, and trouble signals to the monitoring station, operating over a standard voice grade telephone leased line. Comply with UL 1635.

K. Printout of Events: On receipt of signal, print alarm, supervisory, and trouble events. Identify zone, device, and function. Include type of signal (alarm, supervisory, or trouble) and date and time of occurrence. Differentiate alarm signals from all other printed indications. Also print system reset event, including same information for device, location, date, and time. Commands initiate the printing of a list of existing alarm, supervisory, and trouble conditions in the system and a historical log of events.

2.10 AUDIBLE AND VISUAL ALARM DEVICES

A. Basis-of-Design Product: Subject to compliance with requirements, provide product by one of the following:

1. Alarm Controls Corporation.
2. Cooper Wheelock.
3. Edwards Signaling & Security Systems; part of GE Security.
4. Honeywell International Inc.; Honeywell Security.
5. Potter Electric Signal, LLC.

B. Siren: 30-W speaker with siren driver, rated to produce a minimum sound output of 103 dB at 10 feet (3 m) from master control unit.

1. Enclosure: Weather-resistant steel box with tamper switches on cover and on back of box.

C. Strobe: Xenon light complying with UL 1638, with a clear polycarbonate lens.

1. Light Output: 115 cd, minimum.
2. Flash Rate: 60 per minute.

2.11 SECURITY FASTENERS

A. Operable only by tools produced for use on specific type of fastener by fastener manufacturer or other licensed fabricator. Drive system type, head style, material, and protective coating as required for assembly, installation, and strength.

B. Basis-of-Design Product: Subject to compliance with requirements, provide product by one of the following:

1. Acument Global Technologies North America.
2. Safety Socket LLC.
3. Tamper-Pruf Screws.

C. Drive System Types: Pinned Torx-Plus.

D. Socket Flat Countersunk Head Fasteners:

1. Heat-treated alloy steel, ASTM F 835 (ASTM F 835M).
2. Stainless steel, ASTM F 879 (ASTM F 879M), Group 1 CW.

E. Socket Button Head Fasteners:

1. Heat-treated alloy steel, ASTM F 835 (ASTM F 835M).
2. Stainless steel, ASTM F 879 (ASTM F 879M), Group 1 CW.

F. Socket Head Cap Fasteners:

1. Heat-treated alloy steel, ASTM A 574 (ASTM A 574M).
2. Stainless steel, ASTM F 837 (ASTM F 837M), Group 1 CW.

G. Protective Coatings for Heat-Treated Alloy Steel:

1. Zinc chromate, ASTM F 1135, Grade 3 or Grade 4, for exterior applications and interior applications where indicated.
2. Zinc phosphate with oil, ASTM F 1137, Grade I, or black oxide unless otherwise indicated.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Examine substrates, areas, and conditions, with Installer present, for compliance with requirements for installation tolerances and other conditions affecting performance of intrusion detection.

B. Examine roughing-in for embedded and built-in anchors to verify actual locations of intrusion detection connections before intrusion detection installation.

C. Prepare written report, endorsed by Installer, listing conditions detrimental to performance of intrusion detection.

D. Inspect built-in and cast-in anchor installations, before installing intrusion detection, to verify that anchor installations comply with requirements. Prepare inspection reports.

1. Remove and replace anchors where inspections indicate that they do not comply with requirements. Reinspect after repairs or replacements are made.
2. Perform additional inspections to determine compliance of replaced or additional anchor installations. Prepare inspection reports.

E. For material whose orientation is critical for its performance as a ballistic barrier, verify installation orientation.

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

3.2 SYSTEM INSTALLATION

A. Comply with UL 681 and NFPA 731.

B. Equipment Mounting: Install master control unit on finished floor with tops of cabinets not more than 72 inches (1830 mm) above the finished floor.

1. Comply with requirements for seismic-restraint devices specified in Division 26 Section "Vibration and Seismic Controls for Electrical Systems."

C. Install wall-mounted equipment, with tops of cabinets not more than 72 inches (1830 mm) above the finished floor.

1. Comply with requirements for seismic-restraint devices specified in Division 26 Section "Vibration and Seismic Controls for Electrical Systems."

D. Connecting to Existing Equipment: Verify that existing perimeter security system is operational before making changes or connections.

1. Connect new equipment to existing control panel in existing part of the building.

2. Connect new equipment to existing monitoring equipment at the Supervising Station.

3. Expand, modify, and supplement existing monitoring equipment as necessary to extend existing control and monitoring functions to the new points. New components shall be capable of merging with existing configuration without degrading the performance of either system.

E. Security Fasteners: Where accessible to inmates, install intrusion detection components using security fasteners with head style appropriate for fabrication requirements, strength, and finish of adjacent materials except that a maximum of two different sets of tools shall be required to operate security fasteners for Project. Provide stainless-steel security fasteners in stainless-steel materials.

3.3 WIRING INSTALLATION

A. Wiring Method: Install wiring in metal raceways according to Division 26 Section "Raceway and Boxes for Electrical Systems." Conceal raceway except in unfinished spaces and as indicated. Minimum conduit size shall be 3/4 inch. Control and data transmission wiring shall not share conduit with other building wiring systems.

B. Wiring Method: Install wiring in metal raceways according to Division 26 Section "Raceway and Boxes for Electrical Systems," except in accessible indoor ceiling spaces and in interior hollow gypsum board partitions where cable may be used. Conceal raceways and wiring except in unfinished spaces and as indicated. Minimum conduit size shall be 3/4 inch. Control and data transmission wiring shall not share conduit with other building wiring systems.

C. Wiring Method: Cable, concealed in accessible ceilings, walls, and floors when possible.

D. Wiring within Enclosures: Bundle, lace, and train conductors to terminal points. Use lacing bars and distribution spools. Separate power-limited and non-power-limited conductors as recommended in writing by manufacturer. Install conductors parallel with or at right angles to sides and back of enclosure. Connect conductors that are terminated, spliced, or interrupted in any enclosure associated with intrusion system to terminal blocks. Mark each terminal according to system's wiring diagrams. Make all connections with approved crimp-on terminal spade lugs, pressure-type terminal blocks, or plug connectors.

E. Wires and Cables:

1. Conductors: Size as recommended in writing by system manufacturer unless otherwise indicated.

2. 120-V Power Wiring: Install according to Division 26 Section "Low-Voltage Electrical Power Conductors and Cables" unless otherwise indicated.

3. Control and Signal Transmission Conductors: Install unshielded, twisted-pair cable unless otherwise indicated or if manufacturer recommends shielded cable, according to Division 28 Section "Conductors and Cables for Electronic Safety and Security."

4. Data and Television Signal Transmission Cables: Install according to Division 28 Section "Conductors and Cables for Electronic Safety and Security."

F. Splices, Taps, and Terminations: Make connections only on numbered terminal strips in junction, pull, and outlet boxes; terminal cabinets; and equipment enclosures.

G. Install power supplies and other auxiliary components for detection devices at control units unless otherwise indicated or required by manufacturer. Do not install such items near devices they serve.

H. Identify components with engraved, laminated-plastic or metal nameplate for master control unit and each terminal cabinet, mounted with corrosion-resistant screws. Nameplates and label products are specified in Division 26 Section "Identification for Electrical Systems."

3.4 IDENTIFICATION

A. Identify system components, wiring, cabling, and terminals. Comply with identification requirements in Division 26 Section "Identification for Electrical Systems."

B. Install instructions frame in a location visible from master control unit.

3.5 GROUNDING

A. Ground the master control unit and associated circuits; comply with IEEE 1100. Install a ground wire from main service ground to master control unit.

B. Ground system components and conductor and cable shields to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

C. Signal Ground Terminal: Locate at main equipment rack or cabinet. Isolate from power system and equipment grounding. Provide 5-ohm ground. Measure, record, and report ground resistance.

D. Install grounding electrodes of type, size, location, and quantity indicated. Comply with installation requirements in Division 26 Section "Grounding and Bonding for Electrical Systems."

3.6 FIELD QUALITY CONTROL

A. Pretesting: After installation, align, adjust, and balance system and perform complete pretesting to determine compliance of system with requirements in the Contract Documents. Correct deficiencies observed in pretesting. Replace malfunctioning or damaged items with new ones and retest until satisfactory performance and conditions are achieved. Prepare forms for systematic recording of acceptance test results.

1. Report of Pretesting: After pretesting is complete, provide a letter certifying that installation is complete and fully operable; include names and titles of witnesses to preliminary tests.

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

C. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect, test, and adjust components, assemblies, and equipment installations, including connections.

D. Perform tests and inspections.

1. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.

E. Tests and Inspections: Comply with provisions in NFPA 731, Ch. 9, "Testing and Inspections."

1. Inspection: Verify that units and controls are properly labeled and interconnecting wires and terminals are identified.

2. Test Methods: Intrusion detection systems and other systems and equipment that are associated with detection and accessory equipment shall be tested according to Table "Test Methods" and Table "Test Methods of Initiating Devices."

F. Documentation: Comply with provisions in NFPA 731, Ch. 4, "Documentation."

G. Tag all equipment, stations, and other components for which tests have been satisfactorily completed.

3.7 ADJUSTING

A. Occupancy Adjustments: When requested within 2 months of date of Substantial Completion, provide on-site assistance in adjusting system to suit actual occupied conditions. Provide up to three visits to Project during other-than-normal occupancy hours for this purpose. Visits for this purpose shall be in addition to any required by warranty.

3.8 DEMONSTRATION

A. Engage a factory-authorized service representative to train Owner's maintenance personnel to adjust, operate, and maintain the intrusion detection system. Comply with documentation provisions in NFPA 731, Ch. 4, "Documentation and User Training."

***** END OF SECTION *****

THIS PAGE IS INTENTIONALLY BLANK

SECTION 28 23 00

VIDEO SURVEILLANCE

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

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

1.3 DEFINITIONS

A. AGC: Automatic gain control.

B. BNC: Bayonet Neill-Concelman - type of connector.

C. B/W: Black and white.

D. CCD: Charge-coupled device.

E. FTP: File transfer protocol.

F. IP: Internet protocol.

G. LAN: Local area network.

H. MPEG: Moving picture experts group.

I. NTSC: National Television System Committee.

J. PC: Personal computer.

K. PTZ: Pan-tilt-zoom.

L. RAID: Redundant array of independent disks.

M. TCP: Transmission control protocol - connects hosts on the Internet.

N. UPS: Uninterruptible power supply.

O. WAN: Wide area network.

1.4 PERFORMANCE REQUIREMENTS

A. Seismic Performance: Video surveillance system shall withstand the effects of earthquake motions determined according to ASCE/SEI 7.

1. The term "withstand" means "the unit will remain in place without separation of any parts from the device when subjected to the seismic forces specified and the unit will be fully operational after the seismic event."

1.5 SUBMITTALS

A. Product Data: For each type of product indicated. Include dimensions and data on features, performance, electrical characteristics, ratings, and finishes.

B. Shop Drawings: For video surveillance. Include plans, elevations, sections, details, and attachments to other work.

1. Detail equipment assemblies and indicate dimensions, weights, loads, required clearances, method of field assembly, components, and location and size of each field connection.

2. Functional Block Diagram: Show single-line interconnections between components for signal transmission and control. Show cable types and sizes.

3. Dimensioned plan and elevations of equipment racks, control panels, and consoles. Show access and workspace requirements.

4. UPS: Sizing calculations.

5. Wiring Diagrams: For power, signal, and control wiring.

C. Equipment List: Include every piece of equipment by model number, manufacturer, serial number, location, and date of original installation. Add pretesting record of each piece of equipment, listing name of person testing, date of test, set points of adjustments, name and description of the view of preset positions, description of alarms, and description of unit output responses to an alarm.

D. Seismic Qualification Certificates: For video surveillance, cameras, camera-supporting equipment, accessories, and components, from manufacturer.

1. Basis for Certification: Indicate whether withstand certification is based on actual test of assembled components or on calculation.

2. Dimensioned Outline Drawings of Equipment Unit: Identify center of gravity and locate and describe mounting and anchorage provisions.

3. Detailed description of equipment anchorage devices on which the certification is based and their installation requirements.

E. Field quality-control reports.

F. Operation and Maintenance Data: For cameras, power supplies, infrared illuminators, monitors, videotape recorders, digital video recorders, video switches, and control-station components to include in emergency, operation, and maintenance manuals. In addition to items specified in Division 01 Section "Operation and Maintenance Data," include the following:

1. Lists of spare parts and replacement components recommended to be stored at the site for ready access.

G. Warranty: Sample of special warranty.

1.6 QUALITY ASSURANCE

A. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

B. Comply with NECA 1.

C. Comply with NFPA 70.

D. Electronic data exchange between video surveillance system with an access-control system shall comply with SIA TVAC.

1.7 PROJECT CONDITIONS

A. Environmental Conditions: Capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:

1. Control Station: Rated for continuous operation in ambient temperatures of 60 to 85 deg F (16 to 29 deg C) and a relative humidity of 20 to 80 percent, noncondensing.

2. Interior, Controlled Environment: System components, except central-station control unit, installed in air-conditioned interior environments shall be rated for continuous operation in

ambient temperatures of 36 to 122 deg F (2 to 50 deg C) dry bulb and 20 to 90 percent relative humidity, noncondensing. Use NEMA 250, Type 1 enclosures.

3. Interior, Uncontrolled Environment: System components installed in non-air-conditioned interior environments shall be rated for continuous operation in ambient temperatures of 0 to 122 deg F (minus 18 to plus 50 deg C) dry bulb and 20 to 90 percent relative humidity, noncondensing. Use NEMA 250, Type 3R enclosure.

4. Exterior Environment: System components installed in locations exposed to weather shall be rated for continuous operation in ambient temperatures of minus 30 to plus 122 deg F (minus 34 to plus 50 deg C dry bulb and 20 to 90 percent relative humidity, condensing. Rate for continuous operation when exposed to rain as specified in NEMA 250, winds up to 110 mph. Use NEMA 250, Type 3R enclosure.

5. Security Environment: Camera housing for use in outdoor areas where surveillance equipment may be subject to physical violence.

1.8 WARRANTY

A. Special Warranty: Manufacturer's standard form in which manufacturer agrees to repair or replace components of cameras, equipment related to camera operation, and control-station equipment that fail in materials or workmanship within specified warranty period.

1. Warranty Period: Three years from date of Substantial Completion.

PART 2 - PRODUCTS

2.1 SYSTEM REQUIREMENTS

A. Video-signal format shall comply with NTSC standard, composite interlaced video. Composite video-signal termination shall be 75 ohms.

B. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor's entry connection to components.

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

2.2 STANDARD CAMERAS

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. AXCESS International Inc.

2. Bosch Security Systems, Inc.

3. CBC (AMERICA) Corp.

4. COP-USA.

5. Crest Electronics, Inc.

6. Elbex Ltd.; Elbex America Inc.

7. ELMO.

8. EverFocus Electronics Corporation.

9. GENWAC; a brand of Watec Cameras.

10. GE Security, Inc.
11. Hitachi, Ltd.
12. Honeywell International Inc.; Honeywell Video Systems.
13. Hunt Electronics USA, Inc.
14. Ikegami Electronics (USA) Inc.
15. JVC Americas Corp.; JVC Professional products.
16. Merit Li-Lin (USA) Corp.
17. Panasonic Corporation of North America; Panasonic Security Systems.
18. Pelco.
19. Pixera Corporation.
20. Safety Vision.
21. Samsung Opto-Electronics.
22. SANYO North America Corporation.
23. Telpix Electronics, Inc.
24. Toshiba Corporation; Surveillance products.
25. Trinus Systems Inc.
26. Tyco International Limited; Sensormatic products.
27. VELTEK.
28. Vicon Industries, Inc.
29. Videology Imaging Solutions, Inc.
30. Visiontech.
31. Watec America Corporation.

B. Automatic Color Dome Camera: Assembled and tested as a manufactured unit, containing dome assembly, color camera, motorized pan and tilt, zoom lens, and receiver/driver.

1. Comply with UL 639.
2. Pickup Device: CCD interline transfer, 380,000 768(H) by 494(V) pixels.
3. Horizontal Resolution: 480 lines.
4. Signal-to-Noise Ratio: Not less than 50 dB, with camera AGC off.
5. With AGC, manually selectable on or off.
6. Sensitivity: Camera shall provide usable images in low-light conditions, delivering an image at a scene illumination of 6 lux at f/2.0 with camera AGC off.
7. Sensitivity: Camera shall deliver 1-V peak-to-peak video signal at the minimum specified light level. Illumination for the test shall be with lamps rated at approximately 2200-K color temperature, and with camera AGC off.
8. Manually selectable modes for backlight compensation or normal lighting.
9. Pan and Tilt: Direct-drive motor, 360-degree rotation angle, and 180-degree tilt angle. Pan-and-tilt speed shall be controlled by operator. Movement from preset positions shall be not less than 300 degrees per second.

10. Preset Positioning: Eight user-definable scenes, each allowing 16-character titles. Controls shall include the following:

    a. In "sequence mode," camera shall continuously sequence through preset positions, with dwell time and sequencing under operator control.

    b. Motion detection shall be available at each camera position.

    c. Up to four preset positions may be selected to be activated by an alarm. Each of the alarm positions may be programmed to output a response signal.

11. Scanning Synchronization: Determined by external synch over the coaxial cable. Camera shall revert to internally generated synchronization on loss of external synch signal.

12. White Balance: Auto-tracing white balance, with manually settable fixed balance option.

13. Motion Detector: Built-in digital.

14. Dome shall support multiplexed control communications using coaxial cable recommended by manufacturer.

2.3 REINFORCED DOME CAMERAS

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. Extreme CCTV Surveillance Systems.

B. Camera: Designed for high-abuse locations, with a weathertight surface mounting, impact-resistance polycarbonate dome, and heavy-gage, 6061 T6 aluminum body.

1. Suitable for exterior environment, rated for continuous operation in ambient temperatures of minus 40 to plus 122 deg F (minus 40 to plus 50 deg C) dry bulb and up to 85 percent relative humidity.

2. Pickup Device: CCD interline transfer, 290,000 510(H) by 492(V) pixels.

3. Horizontal Resolution: 350 lines.

4. Signal-to-Noise Ratio: Not less than 46 dB.

5. With AGC and automatic backlight compensation.

6. Sensitivity: Camera shall provide usable images in low-light conditions, delivering an image at a scene illumination of 6 lux at f/2.0.

7. Scanning Synchronization: Determined by external synch over the coaxial cable. Camera shall revert to internally generated synchronization on loss of external synch signal.

8. White Balance: Auto-tracing white balance.

2.4 LENSES

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. Bosch Security Systems, Inc.

2. CBC (AMERICA) Corp.

3. COP-USA.

4. Crest Electronics, Inc.

5. Elbex Ltd.; Elbex America Inc.
6. GENWAC; a brand of Watec Cameras.
7. GE Security, Inc.
8. Hitachi, Ltd.
9. Honeywell International Inc.; Honeywell Video Systems.
10. Hunt Electronics USA, Inc.
11. International Space Optics; Rainbow CCTV products.
12. Panasonic Corporation of North America; Panasonic Security Systems.
13. Pelco.
14. Samsung Opto-Electronics.
15. SANYO North America Corporation.
16. Tamron USA, Inc.; Industrial Optics Division.
17. Telpix Electronics, Inc.
18. Tyco International Limited; Sensormatic products.
19. VELTEK.
20. Vicon Industries, Inc.
21. Videology Imaging Solutions, Inc.
22. Watec America Corporation.

B. Description: Optical-quality coated lens, designed specifically for video-surveillance applications and matched to specified camera. Provide color-corrected lenses with color cameras.

1. Auto-Iris Lens: Electrically controlled iris with circuit set to maintain a constant video level in varying lighting conditions.
2. Fixed Lens: With calibrated focus ring.
3. Zoom Lens: Motorized, remote-controlled unit, rated as "quiet operating." Features include the following:
    a. Electrical Leads: Filtered to minimize video signal interference.
    b. Motor Speed: Variable.
    c. Lens shall be available with preset positioning capability to recall the position of specific scenes.

2.5 POWER SUPPLIES

A. Low-voltage power supplies matched for voltage and current requirements of cameras and accessories, and of type as recommended by manufacturer of camera, infrared illuminator, and lens.

1. Enclosure: NEMA 250, Type 3R

2.6 CAMERA-SUPPORTING EQUIPMENT

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. Bosch Security Systems, Inc.

2. CBC (AMERICA) Corp.
3. COP-USA.
4. Crest Electronics, Inc.
5. Elbex Ltd.; Elbex America Inc.
6. ELMO.
7. EverFocus Electronics Corporation.
8. GENWAC; a brand of Watec Cameras.
9. GE Security, Inc.
10. Honeywell International Inc.; Honeywell Video Systems.
11. Ikegami Electronics (USA) Inc.
12. Merit Li-Lin (USA) Corp.
13. Panasonic Corporation of North America; Panasonic Security Systems.
14. Pelco.
15. Samsung Opto-Electronics.
16. SANYO North America Corporation.
17. Telpix Electronics, Inc.
18. Tyco International Limited; Sensormatic products.
19. VELTEK.
20. Vicon Industries, Inc.
21. Videolarm.
22. Video Mount Products.
23. Visiontech.
24. Wren Associates Limited.

B. Minimum Load Rating: Rated for load in excess of the total weight supported times a minimum safety factor of two.

C. Pan-and-Tilt Units: Motorized units arranged to provide remote-controlled aiming of cameras with smooth and silent operation, and equipped with matching mounting brackets.

1. Panning Rotation: 0 to 355 degrees, with adjustable stops.
2. Tilt Movement: 90 degrees, plus or minus 5 degrees, with adjustable stops.
3. Speed: 12 degrees per second in both horizontal and vertical planes.
4. Wiring: Factory prewired for camera and zoom lens functions and pan-and-tilt power and control.
5. Built-in encoders or potentiometers for position feedback, and thermostat-controlled heater.
6. Pan-and-tilt unit shall be available with preset positioning capability to recall the position of a specific scene.

D. Mounting Brackets for Fixed Cameras: Type matched to items supported and mounting conditions. Include manual pan-and-tilt adjustment.

E. Protective Housings for Fixed and Movable Cameras: Steel or 6061 T6 aluminum enclosures with internal camera mounting and connecting provisions that are matched to camera/lens combination and mounting and installing arrangement of camera to be housed.

1. Tamper switch on access cover sounds an alarm signal when unit is opened or partially disassembled. Central-control unit shall identify tamper alarms and indicate location in alarm display. Tamper switches and central-control unit are specified in Division 28 Section "Intrusion Detection."
2. Camera Viewing Window: Lexan window, aligned with camera lens.
3. Duplex Receptacle: Internally mounted.
4. Alignment Provisions: Camera mounting shall provide for field aiming of camera and permit removal and reinstallation of camera lens without disturbing camera alignment.
5. Built-in, thermostat-activated heater and blower units. Units shall be automatically controlled so the environmental limits of the camera equipment are not exceeded.
6. Sun shield shall not interfere with normal airflow around the housing.
7. Mounting bracket and hardware for wall or ceiling mounting of the housing. Bracket shall be of same material as the housing; mounting hardware shall be stainless steel.
8. Finish: Housing and mounting bracket shall be factory finished using manufacturer's standard finishing process suitable for the environment.
9. Enclosure Rating: NEMA Type 3R.

2.7 MONITORS

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. Bosch Security Systems, Inc.
2. CBC (AMERICA) Corp.
3. COP-USA.
4. Crest Electronics, Inc.
5. Elbex Ltd.; Elbex America Inc.
6. ELMO.
7. EverFocus Electronics Corporation.
8. GENWAC; a brand of Watec Cameras.
9. GE Security, Inc.
10. Hitachi, Ltd.
11. Honeywell International Inc.; Honeywell Video Systems.
12. Hunt Electronics USA, Inc.
13. Ikegami Electronics (USA) Inc.
14. International Space Optics; Rainbow CCTV products.
15. JVC Americas Corp.; JVC Professional products.
16. Merit Li-Lin (USA) Corp.
17. Panasonic Corporation of North America; Panasonic Security Systems.